AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 112–403

TEN YEARS AFTER 9/11 — 2011

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

A REPORT FROM THE 9/11 COMMISSION CHAIRMEN—MARCH 30, 2011

IS INTELLIGENCE REFORM WORKING?—PART I—MAY 12, 2011

IS INTELLIGENCE REFORM WORKING?—PART II—MAY 19, 2011

NEXT STEPS FOR SECURING RAIL AND TRANSIT—JUNE 22, 2011

PREVENTING TERRORIST TRAVEL—JULY 13, 2011

IMPROVING EMERGENCY COMMUNICATIONS—JULY 27, 2011

SUCCESSFUL REFORMS AND CHALLENGES AHEAD AT THE DEPARTMENT OF HOMELAND SECURITY—SEPTEMBER 7, 2011

ARE WE SAFER?—SEPTEMBER 13, 2011

A STATUS REPORT ON INFORMATION SHARING—OCTOBER 12, 2011

PROTECTING AGAINST BIOLOGICAL THREATS—OCTOBER 18, 2011

THE NEXT WAVE IN AVIATION SECURITY—NOVEMBER 2, 2011

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

67–123 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

TEN YEARS AFTER 9/11 — 2011

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00002 Fmt 6019 Sfmt 6019 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

S. Hrg. 112–403

TEN YEARS AFTER 9/11 — 2011

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

A REPORT FROM THE 9/11 COMMISSION CHAIRMEN—MARCH 30, 2011

IS INTELLIGENCE REFORM WORKING?—PART I—MAY 12, 2011

IS INTELLIGENCE REFORM WORKING?—PART II—MAY 19, 2011

NEXT STEPS FOR SECURING RAIL AND TRANSIT—JUNE 22, 2011

PREVENTING TERRORIST TRAVEL—JULY 13, 2011

IMPROVING EMERGENCY COMMUNICATIONS—JULY 27, 2011

SUCCESSFUL REFORMS AND CHALLENGES AHEAD AT THE DEPARTMENT OF HOMELAND SECURITY—SEPTEMBER 7, 2011

ARE WE SAFER?—SEPTEMBER 13, 2011

A STATUS REPORT ON INFORMATION SHARING—OCTOBER 12, 2011

PROTECTING AGAINST BIOLOGICAL THREATS—OCTOBER 18, 2011

THE NEXT WAVE IN AVIATION SECURITY—NOVEMBER 2, 2011

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE McCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
SCOTT P. BROWN, Massachusetts
JOHN McCAIN, Arizona
RON JOHNSON, Wisconsin
JOHN ENSIGN, Nevada*
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JERRY MORAN, Kansas**

MICHAEL L. ALEXANDER, *Staff Director*
BETH M. GROSSMAN, *Deputy Staff Director and Chief Counsel*
MARY BETH SCHULTZ, *Associate Staff Director and Chief Counsel for Homeland Security Preparedness and Response*
GORDON N. LEDERMAN, *Associate Staff Director and Chief Counsel for National Security and Investigations*
CHRISTIAN J. BECKNER, *Associate Staff Director for Homeland Security Prevention and Protection*
TROY H. CRIBB, *Senior Counsel*
JEFFREY D. RATNER, *Counsel*
JASON M. YANUSSI, *Senior Professional Staff Member*
SEAMUS A. HUGHES, *Professional Staff Member*
AARON M. FIROVED, *Professional Staff Member*
ELYSE F. GREENWALD, *Professional Staff Member*
ALFRED CUMMING, *Senior Investigator*
ROBERT H. BRADLEY, *Staff Assistant*
NICHOLAS A. ROSSI, *Minority Staff Director*
MOLLY A. WILKINSON, *Minority General Counsel*
BRENDAN P. SHIELDS, *Minority Director of Homeland Security Policy*
LUKE P. BELLOCCHI, *Minority Counsel*
ERIC B. HEIGHBERGER, *Minority Professional Staff Member*
JARED F. GOLDEN, *Minority Professional Staff Member*
HEATHER E. RAITI, *Minority Professional Staff Member*
SCOTT K. LEMASTERS, *Minority U.S. Coast Guard Detailee*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk*
LAURA W. KILBRIDE, *Hearing Clerk*

*Senator Ensign resigned on May 3, 2011.
**Senator Moran joined the Committee on May 11, 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00004 Fmt 5904 Sfmt 5904 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

CONTENTS

Page

WEDNESDAY, MARCH 30, 2011

Opening statements:
- Senator Lieberman 1
- Senator Collins 4
- Senator McCain 6
- Senator Akaka 18
- Senator Carper 20

Prepared statements:
- Senator Lieberman 359
- Senator Collins 361

WITNESSES

Hon. Thomas H. Kean, Former Chairman of the National Commission on Terrorist Attacks Upon the United States 6

Hon. Lee H. Hamilton, Former Vice Chairman of the National Commission on Terrorist Attacks Upon the United States 9

ALPHABETICAL LIST OF WITNESSES

Kean, Hon. Thomas H.:
- Testimony 6
- Prepared statement 364

Hamilton, Hon. Lee H.:
- Testimony 9
- Prepared statement 364

APPENDIX

Letter to the President of the United States, dated April 8, 2011, submitted for the Record by Senator Lieberman 387

Responses to post-hearing questions for the Record from:
- Mr. Kean and Mr. Hamilton 389

THURSDAY, MAY 12, 2011

Opening statements:
- Senator Lieberman 31
- Senator Collins 32

Prepared statements:
- Senator Lieberman 395
- Senator Collins 398

WITNESSES

Hon. Jane Harman, Former Representative from California and Chair of the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment 34

Hon. Michael V. Hayden, Former Director of the Central Intelligence Agency and Former Director of the National Security Agency 37

John C. Gannon, Former Deputy Director for Intelligence at the Central Intelligence Agency 40

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00005 Fmt 5904 Sfmt 5904 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

Page

ALPHABETICAL LIST OF WITNESSES

Gannon, John C.:
Testimony 40
Prepared statement 406
Harman, Hon. Jane:
Testimony 34
Prepared statement 400
Hayden, Hon. Michael V.:
Testimony 37
Prepared statement 403

THURSDAY, MAY 19, 2011

Opening statements:
Senator Lieberman 59
Senator Collins 60
Senator Brown 69
Senator Carper 71
Prepared statements:
Senator Lieberman 412
Senator Collins 414

WITNESS

Hon. Dennis C. Blair, Former Director of National Intelligence:
Testimony 61
Prepared statement 416

WEDNESDAY, JUNE 22, 2011

Opening statements:
Senator Lieberman 83
Senator Collins 85
Senator Paul 101
Senator Landrieu 104
Senator Carper 111
Prepared statements:
Senator Lieberman 436
Senator Collins 438
Senator Landrieu 440

WITNESSES

Hon. John S. Pistole, Administrator, Transportation Security Administration, U.S. Department of Homeland Security 87
Hon. Peter J. Boynton, Commissioner, Connecticut Department of Emergency Management and Homeland Security 90
Stephen E. Flynn, Ph.D., President, Center for National Policy 93

ALPHABETICAL LIST OF WITNESSES

Boynton, Hon. Peter J.:
Testimony 90
Prepared statement 450
Flynn, Ph.D., Stephen E.:
Testimony 93
Prepared statement 454
Pistole, Hon. John S.:
Testimony 87
Prepared statement with an attachment 442

APPENDIX

Brian Michael Jenkins, Director, National Transportation Security Center of Excellence, Mineta Transportation Institute, document submitted for the Record by Senator Lieberman 462
Responses to post-hearing questions for the Record from:
Mr. Pistole 467

Page

Responses to post-hearing questions for the Record from—Continued
Mr. Boynton 485
Mr. Flynn 491

WEDNESDAY, JULY 13, 2011

Opening statements:
Senator Lieberman 117
Senator Collins 120
Senator Paul 136
Senator Brown 141
Prepared statements:
Senator Lieberman 493
Senator Collins 496

WITNESSES

Hon. Rand Beers, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security 122
Hon. Janice L. Jacobs, Assistant Secretary, Bureau of Consular Affairs, U.S. Department of State 124
Hon. David F. Heyman, Assistant Secretary, Office of Policy, U.S. Department of Homeland Security 127

ALPHABETICAL LIST OF WITNESSES

Beers, Hon. Rand:
Testimony 122
Prepared statement 499
Heyman, Hon. David F.:
Testimony 127
Prepared statement 530
Jacobs, Hon. Janice L.:
Testimony 124
Prepared statement 506

APPENDIX

Responses to post-hearing questions for the Record from:
Mr. Beers and Mr. Heyman 542
Ms. Jacobs 568

WEDNESDAY, JULY 27, 2011

Opening statements:
Senator Lieberman 151
Senator Collins 154
Senator Brown 170
Prepared statements:
Senator Lieberman 594
Senator Collins 597

WITNESSES

Gregory Schaffer, Acting Deputy Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security 157
Michael D. Varney, Statewide Interoperability Coordinator, Connecticut Department of Emergency Services and Public Protection 159
Robert P. McAleer, Director, Maine Emergency Management Agency 161
Charles H. Ramsey, Police Commissioner, Philadelphia Police Department 164

ALPHABETICAL LIST OF WITNESSES

McAleer, Robert P.:
Testimony 161
Prepared statement with an attachment 616
Ramsey, Charles H.:
Testimony 164
Prepared statement 627

Page

Schaffer, Gregory:
Testimony 157
Prepared statement 599
Varney, Michael D.:
Testimony 159
Prepared statement 611

APPENDIX

Responses to post-hearing questions for the Record from:
Mr. Schaffer 630

WEDNESDAY, SEPTEMBER 7, 2011

Opening statements:
Senator Lieberman 179
Senator Collins 181
Senator Akaka 193
Senator Pryor 195
Senator Carper 197
Prepared statements:
Senator Lieberman 641
Senator Collins 644

WITNESSES

Hon. Jane Holl Lute, Deputy Secretary, U.S. Department of Homeland Security 183
Hon. Eugene L. Dodaro, Comptroller General of the United States, U.S. Government Accountability Office, accompanied by Cathleen A. Berrick, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office 185

ALPHABETICAL LIST OF WITNESSES

Dodaro, Hon. Eugene L.:
Testimony 185
Prepared statement with an attachment 660
Lute, Hon. Jane Holl:
Testimony 183
Prepared statement 647

APPENDIX

Report to Congressional Requesters titled, "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11," submitted by Mr. Dodaro 689
Responses to post-hearing questions for the Record from:
Ms. Lute 894

TUESDAY, SEPTEMBER 13, 2011

Opening statements:
Senator Lieberman 207
Senator Collins 208
Senator Brown 224
Senator Carper 227
Senator Johnson 230
Senator Moran 232
Senator McCain 233
Senator Akaka 236
Senator Paul 238
Senator Levin 241
Prepared statements:
Senator Lieberman 912
Senator Collins 914
Senator Moran 917

Page

WITNESSES

Hon. Janet A. Napolitano, Secretary, U.S. Department of Homeland Security . 211
Hon. Robert S. Mueller III, Director, Federal Bureau of Investigation, U.S. Department of Justice 214
Hon. Matthew G. Olsen, Director, National Counterterrorism Center, Office of the Director of National Intelligence 216

ALPHABETICAL LIST OF WITNESSES

Mueller III, Hon. Robert S.:
Testimony 214
Prepared statement 943
Napolitano, Hon. Janet A.:
Testimony 211
Prepared statement 918
Olsen, Hon. Matthew G.:
Testimony 216
Prepared statement 955

APPENDIX

Anti-Defamation League, letter dated September 14, 2011, with an attachment 966
Margaret Huang, Executive Director, Rights Working Group, prepared statement 981
Hon. John D. Rockefeller IV, a U.S. Senator from the State of West Virginia, prepared statement 994
Responses to post-hearing questions for the Record from:
Secretary Napolitano 996
Mr. Mueller 1045
Mr. Olsen 1053

WEDNESDAY, OCTOBER 12, 2011

Opening statements:
Senator Lieberman 253
Senator Collins 255
Prepared statements:
Senator Lieberman 1061
Senator Collins 1063

WITNESSES

Hon. John E. McLaughlin, Distinguished Practitioner-In-Residence, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University . 257
Hon. Thomas E. McNamara, Adjunct Professor, Elliott School of International Affairs, George Washington University 260
Cathy L. Lanier, Chief of Police, Metropolitan Police Department, District of Columbia 262
Ronald E. Brooks, Director, Northern California Regional Intelligence Center 264
Jeffrey H. Smith, Partner, Arnold and Porter 267

ALPHABETICAL LIST OF WITNESSES

Brooks, Ronald E.:
Testimony 264
Prepared statement 1085
Lanier, Cathy L.:
Testimony 262
Prepared statement 1078
McLaughlin, Hon. John E.:
Testimony 257
Prepared statement 1065
McNamara, Hon. Thomas E.:
Testimony 260
Prepared statement 1073
Smith, Jeffrey H.:
Testimony 267

Page

Smith, Jeffrey H.—Continued
Prepared statement 1107

APPENDIX

Eileen R. Larence, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office, prepared statement 1115
Responses to post-hearing questions for the Record from:
Mr. McLaughlin 1134
Mr. McNamara 1136
Ms. Lanier 1137
Mr. Brooks 1139
Mr. Smith 1142

TUESDAY, OCTOBER 18, 2011

Opening statements:
Senator Lieberman 281
Senator Collins 284
Senator Akaka 300
Prepared statements:
Senator Lieberman 1144
Senator Collins 1147

WITNESSES

Hon. Tara J. O'Toole, Under Secretary for Science and Technology, U.S. Department of Homeland Security 286
Hon. Alexander G. Garza, Assistant Secretary for Health Affairs and Chief Medical Officer, U.S. Department of Homeland Security 289
Hon. Nicole Lurie, Assistant Secretary for Preparedness and Response, U.S. Department of Health and Human Services 291
Vahid Majidi, Ph.D., Assistant Director, Weapons of Mass Destruction Directorate, Federal Bureau of Investigation, U.S. Department of Justice 294
Thomas V. Inglesby, M.D., Director and Chief Executive Officer, Center for Biosecurity, University of Pittsburgh Medical Center 307
Robert P. Kadlec, M.D., Former Special Assistant to the President for Homeland Security and Senior Director for Biological Defense Policy 310
Jeffrey Levi, Ph.D., Executive Director, Trust for America's Health 312

ALPHABETICAL LIST OF WITNESSES

Garza, Hon. Alexander G.:
Testimony 289
Prepared statement 1161
Inglesby, M.D., Thomas V.:
Testimony 307
Prepared statement 1196
Kadlec, M.D., Robert P.:
Testimony 310
Prepared statement 1205
Levi, Ph.D., Jeffrey:
Testimony 312
Prepared statement 1213
Lurie, Hon. Nicole:
Testimony 291
Prepared statement 1167
Majidi, Ph.D., Vahid:
Testimony 294
Prepared statement 1186
O'Toole, Hon. Tara J.:
Testimony 286
Prepared statement 1150

APPENDIX

Responses to post-hearing questions for the Record from:
Dr. Garza 1219

Page

Responses to post-hearing questions for the Record from—Continued
Dr. Lurie 1220

WEDNESDAY, NOVEMBER 2, 2011

Opening statements:
Senator Collins 323
Senator Lieberman 329
Senator Paul 330
Senator Akaka 335
Senator Pryor 336
Senator Moran 351
Senator Landrieu 353
Senator Carper 356
Prepared statements:
Senator Lieberman 1224
Senator Collins 1226
Senator Landrieu 1228

WITNESSES

Hon. John S. Pistole, Administrator, Transportation Security Administration, U.S. Department of Homeland Security 325
Roger J. Dow, President and Chief Executive Officer, U.S. Travel Association . 340
Kenneth J. Dunlap, Global Director, Security and Travel Facilitation, International Air Transport Association 343
Charles M. Barclay, President, American Association of Airport Executives 345

ALPHABETICAL LIST OF WITNESSES

Barclay, Charles M.:
Testimony 345
Prepared statement 1285
Dow, Roger J.:
Testimony 340
Prepared statement 1235
Dunlap, Kenneth J.:
Testimony 343
Prepared statement 1278
Pistole, Hon. John S.:
Testimony 325
Prepared statement 1230

APPENDIX

"A Better Way," a report submitted by Mr. Dow, U.S. Travel Association 1241
Gregory Principato, President, Airports Council International-North America, prepared statement 1292
Donald Lee Moak, President, Air Line Pilots Association International, letter submitted for the Record 1297
Nicholas E. Calio, President and CEO, Air Transport Association, letter submitted for the Record 1301
Marcus W. Flagg, President, Federal Flight Deck Officers Association, prepared statement 1303
Responses to post-hearing questions for the Record from:
Mr. Pistole 1311
Mr. Dow 1332
Mr. Dunlap 1337
Mr. Barclay 1342

Page

ACRONYMS AND ABBREVIATIONS

9/11—September 11, 2001
9/11 Commission—National Commission on Terrorist Attacks Upon the United States
AAAE—American Association of Airport Executives
AIT—Advanced Imaging Technology
AOR—area of responsibility
APEC—Asia-Pacific Economic Cooperation
APIS—Advance Passenger Information System
AQ—al-Qaeda
AQAP—al-Qaeda in the Arabian Peninsula
ASAC—Aviation Security Advisory Committee
ASP—Advanced Spectroscopic Portal
ASPR—Assistant Secretary for Preparedness and Response
ATA—Air Transport Association of America
ATF—Bureau of Alcohol, Tobacco, Firearms and Explosives
ATR—Automated Target Recognition
BARDA—Biomedical Advanced Research Development Authority
BASE—Baseline Assessment for Security Enhancement
BIDP—Border Interoperability Demonstration Project
BRIDGES—Building Respect in Diverse Groups to Enhance Sensitivity
BSL—biosafety level
BTRA—Biothreat Risk Assessment
CAARS—Cargo Advanced Automated Radiography System
CBP—U.S. Customs and Border Protection
CBRN—chemical, biological, radiological, and nuclear
CCTV—closed caption television
CDC—Centers for Disease Control and Prevention
CEO—Chief Executive Officer
CIA—Central Intelligence Agency
CINCPAC—Commander in Chief Pacific Command
CIO—Chief Information Officer
CIS—Citizenship and Immigration Services
CLASS—Closed Loop Artillery Simulation System
CMS—Centers for Medicare and Medicaid Services
CNN—Cable News Network
COML—Communications Unit Leader
COMT—Communications Technician
CRS—Congressional Research Service
CTAB—Counterterrorism Advisory Board
CTC—Counterterrorism Center
CUI—Controlled Unclassified Information
CVE—Countering Violent Extremism
DARPA—Defense Advanced Research Projects Agency
DCA—Ronald Reagan Washington National Airport
DCI—Director of Central Intelligence
DCIA—Director of the Central Intelligence Agency
DEA—Drug Enforcement Administration
DHS—U.S. Department of Homeland Security
DNA—deoxyribonucleic acid
DNA—Defense Nuclear Agency
DNDO—Domestic Nuclear Detection Office
DNI—Director of National Intelligence

Page

DOD—U.S. Department of Defense
DOJ—U.S. Department of Justice
DOT—U.S. Department of Transportation
DTRA—Defense Threat Reduction Agency
ECPC—Emergency Communications Preparedness Center
EMS—emergency medical services
EO—Executive Order
EOC—Emergency Operations Center
EPA—Environmental Protection Agency
ESTA—Electronic System for Travel Authorization
ER—emergency room
FAA—Federal Aviation Administration
FAMS—Federal Air Marshal Service
FBI—Federal Bureau of Investigation
FCC—Federal Communications Commission
FDA—Food and Drug Administration
FEMA—Federal Emergency Management Agency
FISA—Foreign Intelligence Surveillance Act
FOUO—For official use only
FTA—Federal Transit Administration
GAO—U.S. Government Accountability Office
GETS—Government Emergency Telecommunications Service
Haz-Mat—hazardous material
HHS—U.S. Department of Health and Human Services
HIDTA—High Intensity Drug Trafficking Area
HIG—High-Value Interrogation Group
HIV/AIDS—human immunodeficiency virus/acquired immunodeficiency syndrome
HSDN—Homeland Secure Data Network
HVAC—heating, ventilation, and air conditioning
HVE—homegrown violent extremist
I&A—Intelligence and Analysis
IAFIS—Integrated Automated Fingerprint Identification System
IATA—International Air Transport Association
IC—intelligence community
ICAO—International Civil Aviation Organization
ICD—International Classification of Diseases
ICE—U.S. Immigration and Customs Enforcement
ID—identification
IDENT—Automated Biometrics Identification System
IECGP—Interoperable Emergency Communications Grant Program
IED—improvised explosive device
IG—Inspector General
IMF—International Monetary Fund
INA—Immigration and Nationality Act
IPAWS—Integrated Public Alert and Warning System
IRTPA—Intelligence Reform and Terrorism Prevention Act of 2004
ISE—Information Sharing Environment
IT—information technology
ITACG—Interagency Threat Assessment and Coordination Group
IWN—Intergrated Wireless Network
JTTF—Joint Terrorism Task Force
JSOC—Joint Special Operations Command
LAPD—Los Angeles Police Department

Page

LTTE—Liberation Tigers of Tamil Eelam
LWIN—Louisiana Wireless Information Network
MCCA—Major Cities Chiefs Association
MOU—memorandum of understanding
MPD—Metropolitan Police Department
MSCOMMNET—Maine State Communications Network
MTA—Metropolitan Transportation Authority
Navy SEALS—Navy Sea, Air, and Land Teams
NBAF—National Bio- and Agro-Defense Facility
NBIC—National Biosurveillance Integration Center
NBIS—National Biosurveillance Integration System
NCIC—National Crime Information Center
NCR—National Capital Region
NCS—National Communications System
NCSWIC—National Council of Statewide Interoperability Coordinators
NCTC—National Counterterrorism Center
NECP—National Emergency Communications Plan
NGA—National Geospatial-Intelligence Agency
NICS—National Instant Criminal Background Check System
NID—National Intelligence Director
NIEM—National Information Exchange Model
NIH—National Institutes of Health
NIST—National Institute of Standards and Technology
NIP—National Intelligence Program
NPPD—National Protection and Programs Directorate
NSA—National Security Agency
NSC—National Security Council
NSI—National SAR Initiative
NSSE—National Special Security Event
NYPD—New York Police Department
ODNI—Office of the Director of National Intelligence
OEC—Office of Emergency Communications
OHA—Office of Health Affairs
OIG—Office of the Inspector General
OIP—Office of Infrastructure Protection
OMB—Office of Management and Budget
OPCON—Operations Control
OPM—Office of Personnel Management
PAG—Policy Advisory Group
PAHPA—Pandemic and All-Hazards Preparedness Act
PATRIOT Act—Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
PD-DNI—Principal Deputy, Director of National Intelligence
PDB—President's Daily Brief
PERF—Police Executive Research Forum
PETN—pentaerythritol tetranitrate
PHEMCE—Public Health Emergency Medical Countermeasure Enterprise
PNR—passenger name record
PSA—Public Safety Alliance
PSA—public service announcement
PSI—Permanent Subcommittee on Investigations
R&D—Research and Development

Page

RF—radio frequency
RFP—request for proposal
RSO—Regional Security Office
S&T—Science and Technology Directorate
SAFECOM—Emergency communications program of DHS
SAR—suspicious activity reporting
SENTRI—Secure Electronic Network for Travelers Rapid Inspection
SEVIS—Student and Exchange Visitor Information System
SIV—Special Immigrant Visa
SPECTRUM Act—Strengthening Public-Safety and Enhancing Communications Through Reform, Utilization, and Modernization Act
SPP—Screening Partnership Program
SWIC—Statewide Interoperability Coordinator
TACON—tactical control
TASC—Transformation and Systems Consolidation
TEKS—Texas Essential Knowledge and Skills
TIC—Tactical Interoperable Communications
TIP—Terrorist Interdiction Program
TSA—Transportation Security Administration
TTIC—Terrorist Threat Integration Center
TTP—Tehrik-i-Taliban Pakistan (Pakistani Taliban)
TWIC—Transportation Worker Identification Credential
UASI—Urban Areas Security Initiative
UPMC—University of Pittsburgh Medical Center
UPS—United Parcel Service of America, Inc.
US-CERT—U.S. Computer Emergency Readiness Team
USCIS—U.S. Citizenship and Immigration Services
USDA—U.S. Department of Agriculture
USDI—Under Secretary of Defense for Intelligence
USA PATRIOT Act—Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
US-VISIT—U.S. Visitor and Immigrant Status Indicator Technology
VA—Department of Veterans Affairs
VHF—very high frequency
VIPR—Visible Intermodal Prevention and Response
VRVK—visa revoked
VSP—Visa Security Program
VSU—Video Security Unit
WHO—World Health Organization
WIN—Wireless Interoperable Network
WMD—weapons of mass destruction

TEN YEARS AFTER 9/11: A REPORT FROM THE 9/11 COMMISSION CHAIRMEN

WEDNESDAY, MARCH 30, 2011

UNITED STATES SENATE,
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in Room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Carper, Collins, and McCain.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. Thank you all for being here.

The attacks on America by Islamist terrorists on 9/11 took place almost a decade ago, but the memories of that day are still searing. The attacks ended thousands of lives, changed families forever, and forced our country into another worldwide war.

We all remember that morning, and I know we will until the moment we leave Earth. The Nation watched on television as those extraordinary mighty twin towers of the World Trade Center collapsed into a pile of smoking rubble, taking so many innocent lives with them.

American Airlines Flight 77 smashed into the Pentagon and set it ablaze. And in the fields near Shanksville, Pennsylvania, we saw the smoldering crash of United Flight 93, whose brave passengers had fought to retake the plane from the terrorists who had targeted Washington, DC—probably targeted this very place where we are, Capitol Hill—and by their heroism saved hundreds if not thousands of additional lives.

But even as we mourned—and we did—we began to ask—and when I say "we," I mean not just those of us privileged to serve here, but people throughout the country and particularly the families of those who were lost on 9/11—how those attacks could have happened and what could we do to make sure to the best of our ability that nothing like that ever happened again. And so we created the 9/11 Commission to investigate what did happen on 9/11. What were the flaws in our homeland security and what could we do to protect our Nation against another such attack from Islamist terrorists or anyone else who would want to carry out such a dreadful act?

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00017 Fmt 6633 Sfmt 6633 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

Coming to the leadership of that Commission were two extraordinary Americans—gifted, able, and extremely patriotic—Governor Tom Kean and Congressman Lee Hamilton. We are really privileged to have them with us as our witnesses today.

The Commission they led and its staff reviewed 2.5 million pages of documents, interviewed 1,200 individuals in 12 countries—including every relevant senior official of both the Clinton and Bush Administrations—and held 19 days of public hearings across the country with 160 witnesses testifying.

The Commission's recommendations were sweeping and they were definitive. They were not just general conclusions, but they were specific recommendations for both immediate actions we needed to take to defend ourselves against further attack, but also long-term actions we could take to blunt the terrorists' message and dry up their recruitment.

In response to the Commission's recommendations, this Committee authored—and I am honored to see that not only Senator Collins is here but also Senator McCain, three of the four original sponsors of the legislation—the Intelligence Reform and Terrorism Prevention Act of 2004 that adopted not all but most of the recommendations of the 9/11 Commission, including the creation of a Director of National Intelligence and the National Counterterrorism Center, which I thought, and I believe the Commission thought, were the two most substantial and significant recommendations for change it was making.

That Act was the most sweeping reform of our government's intelligence apparatus and, together with the adoption of the Homeland Security Act a couple years before, represented the most significant changes in our governmental framework since the end of World War II.

This Committee was privileged to be deeply involved in drafting these and other pieces of counterterrorism legislation to implement the Commission's recommendations and further strengthen our security against terrorism.

But a lot of the hard work in identifying, recommending, and then adopting the specific reforms was done by the two gentlemen who are testifying before us today: Then the Chairman and Vice Chairman of the 9/11 Commission, now the co-chairmen of its successor, the Bipartisan Policy Center's National Security Preparedness Group. I thank Mr. Kean and Mr. Hamilton for being here today, for their hard work and dedication to public service throughout their lives, and for providing our Nation with a most compelling reminder of how much we can accomplish in public life when we put party labels aside and work together for the national good.

Today, in the exercise of our Committee's responsibility to constantly evaluate and investigate our homeland defenses, and also mindful of the approaching 10th anniversary of the 9/11 attacks, we are beginning a series of oversight hearings on all that we attempted to accomplish after 9/11. Today we are very privileged to have Governor Kean and Congressman Hamilton here to help us begin our review with their opinion of the state of America's homeland security. We have already scheduled four more subject matter hearings for May, June, and July that will look, among other things, at the Office of the Director of National Intelligence, the ef-

fectiveness of our aviation security reforms, what we have done to try to keep terrorists out of the United States, and how we are progressing on the goal that we all said we had to improve, which is emergency communications among law enforcement and associated personnel.

I want to say how grateful I am for the prepared testimony that the two of you have submitted to the Committee, which will be included in full in the record. You have touched on some of the concerns that the Committee has and will deal with in coming hearings. One of the most significant is with regard to the Director of National Intelligence and how that office has done and whether it needs further support to help it achieve the goals that you had for it. Personally, I believe it is essential to have a strong Director of National Intelligence who can marshall the full capabilities of the intelligence community.

I am encouraged by some of the recent changes that the current DNI, General James Clapper, has carried out toward further integration, but I must say I am also concerned about some of the continuing bureaucratic resistance from other components of the intelligence community, which, under our vision and I believe yours, were supposed to be under the supervision of the DNI. I know from your testimony that you both share some of those concerns, and I am interested in hearing your comments on those.

I note with appreciation that you have also talked about the importance of moving more rapidly toward better interoperable communication systems and that one of your recommendations is that we set aside the so-called D Block of the broadband spectrum for funding those public safety improvements. Senator McCain and I sponsored legislation to accomplish that in the last session, and we are working to introduce a similar bill in this session.

So to summarize an awful lot very briefly, I would say that since the 9/11 Commission reforms were adopted, we have seen a very significant improvement in our homeland security. We have had many victories in our battles with terrorists, many plots broken and attacks planned against America thwarted. We have also had some close calls such as the case of the Christmas Day bomber and the other case of the Times Square bomber. And we have had some tragic failures like the homegrown radical Islamist Major Nidal Hasan who murdered 13 Americans at Fort Hood.

So we want to continue to learn from our successes and our failures, and that is the intention of this series of hearings that we are beginning today.

May I say finally that we are very proud and grateful to be joined this morning by some family members of 9/11 victims who went on to become leading advocates for the creation of the 9/11 Commission and the implementation of its recommendations and have continued to play a wonderful oversight role in that work. Mary Fetchet and Carie Lemack are two of the most likable pests we have around Capitol Hill. [Laughter.]

Really, I would say lovable and committed. The Commission would not have been created without their advocacy. We would not have passed its legislative recommendations without their most effective lobbying. And its implementation would not be as good as all of us want it to be if they had not stayed on duty as they have.

So I cannot thank you enough. I know I speak for everybody on the Committee when I express my gratitude and admiration for your personal strength, your skill, and your continuing commitment to America's homeland security.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

This year, we will commemorate the worst attack ever on the United States. In doing so, we must ask ourselves, "Are we safer?" Or are we just safer from the tactics that terrorists already have tried?

Is our intelligence community better at fitting together these complex puzzle pieces? Or have we just been lucky? Are we anticipating the next threat, such as a cyber attack or the use of poisons? Or are we just looking backward, reacting to previous plots?

Undoubtedly, compared to where we were on September 10, 2001, we have greatly improved the framework for information sharing among our intelligence and law enforcement agencies. But sometimes it has been an inept bomb maker or a faulty fuse that has spared American lives.

Once again, the two extraordinary leaders of the landmark 9/11 Commission, Mr. Hamilton and Mr. Kean, are appearing before our Committee as we evaluate our progress in securing our Nation. In September of last year, their "Assessing the Terrorist Threat" report warned of an increasingly wide range of U.S.-based militants who do not fit any particular ethnic, economic, educational, or social profile.

The American melting pot, the report said, "has not provided a firewall against the radicalization and recruitment of American citizens and residents, though it has arguably lulled us into a sense of complacency that homegrown terrorism could not happen in the United States."

This report correctly called 2009 a watershed year in U.S.-based terrorist plots, with 43 American citizens or residents aligned with violent Islamist extremists charged or convicted of terrorist crimes in that year alone.

This Committee first sounded the alarm about home-based terrorism 5 years ago and has held 15 hearings on this topic. We found that individuals within our country, in both our prison system and our communities, are being inspired by al-Qaeda's violent ideology to plan and execute attacks, often acting as "lone wolves" without direct orders or ties to al-Qaeda.

As Senator Lieberman has indicated, the Intelligence Reform and Terrorism Prevention Act of 2004, which we authored, did much to improve the management and performance of our intelligence, homeland security, and law enforcement agencies. This most sweeping reform of our Nation's intelligence community since just after World War II would not have happened without the leadership of our witnesses and the advocacy of the families of the victims. The resulting increased collaboration and information sharing have helped our Nation prevent numerous attacks.

There have been untold successes. In many cases, the intelligence community and law enforcement have quietly connected the

dots and thwarted plots. In other cases, alert citizens have reported suspicious behavior to the authorities just in time.

Challenges still remain, however. We continue to see troubling examples of the pre-9/11 stovepiped mindset from some of our intelligence and law enforcement officers. For example, as documented in our Committee's recent report on the Fort Hood attack, the Army and the FBI collectively had ample information to have detected Major Hasan's radicalization to violent Islamist extremism, but they failed to act on the many red flags signaling that he had become a potential threat.

Major Hasan and others seem to find motivation and ideas online. Technology is transforming our culture, our economy, and our world in many beneficial ways. Yet we must also be alert to the fact that terrorists are seeking to exploit the Internet's potential as well. We have recently witnessed that the Internet can serve as a platform for extremist propaganda on the one hand and peaceful revolution on the other.

Other Commission recommendations have not yet come to fruition, and, of course, the most obvious example of that is Congress' failure to reform itself. But there are others as well. We must make more progress, as the Chairman has indicated, in enhancing first responder communications.

Gaps also remain at our borders and in our cargo inspection systems. As the news today indicates, the potential to plant an explosive somewhere within the millions of pieces of air cargo shipped around the world each day is a real vulnerability.

It is also troubling that the Border Patrol does not have the ability to detect illegal activity across approximately three-quarters of the Northern Border. DHS must continue to work to find a balance that opens our border to our friends while closing it to those who would do us harm.

Nevertheless, there have been real accomplishments: The biometric system for screening foreign nationals seeking to enter the United States, the creation of a consolidated terrorist watchlist, and the dedicated DHS and State and local law enforcement employees all deserve recognition.

But even in these areas of progress, improvements are needed. Biometric screening must be expanded to include foreign nationals leaving the United States. Screening technology must be improved to keep up with changing threats and to ensure that the safest possible screening equipment is deployed.

I hope that this year we can expand protection against lawsuits for citizens who report suspicious behavior indicating potential terrorist activity. We must also pass legislation to ensure that key U.S. intelligence officials are consulted following a foreign terrorist's detention in the United States. That did not happen in the case of Abdulmutallab.

And, finally, I continue to have deep concerns that this Administration refuses to acknowledge that violent Islamist extremism is the ideology that fuels such attacks. The Administration should have an overarching national strategy to counter this growing threat within our own country.

Ten years ago, nearly 3,000 lives were lost on that terrible day. We cannot become complacent or let our guard down when every

single intelligence briefing that I have ever attended always warns that the enemy remains determined to attack our country. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins, for that excellent statement. Normally we limit opening statements to the Chairman and the Ranking Member on the Committee, but Senator McCain was, as you two know, the original sponsor of the legislation that created the 9/11 Commission, so, Senator McCain, I would invite you to make an opening statement if you would like.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. I would just briefly like to thank our witnesses. I think what they did was one of the reasons why this country has not been attacked since 9/11. They are two dedicated public servants, an example of bipartisanship, and I think it is very appropriate that on the 10-year anniversary, we get their continued input. Thank you again for your service to the country.

Chairman LIEBERMAN. Thank you, Senator McCain.

Before we go to the witnesses, I just want to briefly introduce Charles Dowd, Deputy Chief of the New York Police Department for Communications. He has been a very strong proponent of allocating the D Block to public safety, and we appreciate the fact that he is committed enough to this that he is here in the room today.

Governor Kean, welcome, and we look forward to your testimony now.

TESTIMONY OF HON. THOMAS H. KEAN,[1] FORMER CHAIRMAN OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Mr. KEAN. Thank you very much, Mr. Chairman and Senator Collins. We are very pleased to have the opportunity to be here with you once again today. Nobody has been more important than you all have been at the center of defending this country from the terrorist threat that we face. We are deeply grateful for your sustained support of our 9/11 Commission recommendations and your leadership in continuing to reform our national security institutions. Over the last decade, you have done much to ensure that we are taking the difficult steps necessary to confront this determined enemy and protect Americans, our allies, and, for that matter, people throughout the world.

Today, we are appearing in our capacity as co-chairmen of the Bipartisan Policy Center's National Security Preparedness Group. That is the successor organization to the 9/11 Commission. Drawing on a strong roster of national security professionals, we work as an independent, bipartisan group to monitor the implementation of the 9/11 Commission's recommendations and to address other emerging national security issues.

Let me begin by describing the changes in our government since 9/11, the current threat, and perhaps updating you on some of our Commission's recommendations. Lee Hamilton will then continue

[1] The joint prepared statement of Mr. Kean and Mr. Hamilton appears in the Appendix on page 364.

assessing the status of the implementation of a number of these recommendations.

So now nearly 10 years after the tragic 9/11 attacks and 7 years since we finished our report, it really is, as the Committee has decided, a very appropriate time to see just where we are in national security reform and how we are doing.

The terrorist attacks, as everybody knows, had a profoundly dramatic impact on our government, on the private sector, and, for that matter, on our daily lives. The suddenness of that attack on American soil and the loss of so many lives I think made a lot of us feel vulnerable in our homes and caused us to question whether or not our government was properly organized to protect us from this kind of lethal threat. The economic damage resulting from the attacks was severe. Businesses in all sectors have adapted in one way or another to this new reality.

Over the past 10 years, our government's response to the challenge of transnational terrorism has been equally dramatic. We have created major new institutions—the Department of Homeland Security, Cyber Command, and in 2004, with the leadership of Senator Collins and Lieberman, Congress created the Office of the Director of National Intelligence and the National Counterterrorism Center to make sure we had a unity of effort in the intelligence community.

Now, despite all this progress, some major 9/11 Commission recommendations still remain unfulfilled, and we would suggest today that these require urgent action because the threat from al-Qaeda, related terrorist groups, and individual adherents to violent Islamist extremism persists to this day.

Al-Qaeda and related terrorist groups continue to pose a serious threat to all of us. Al-Qaeda Central has been diminished, but its leadership, Osama bin Laden and al-Zawahiri, as we know, are still at large. Although a devastating 9/11-type attack we believe is less likely, the threat is more complex and diverse than at any time in the last decade. Al-Qaeda and its allies continue to have the intent and the reach to kill dozens or even hundreds of Americans in a single attack. There is a high risk of attacks, but we believe that they will likely be smaller.

A key change in recent years is the increasingly prominent role that a number of U.S. citizens and residents have taken in the leadership of al-Qaeda and aligned groups.

Another development is the increasing diversification of the types of U.S.-based jihadist militants. Some are individuals inspired to engage in attacks on their own while others have been actively recruited by overseas terrorist groups. Indeed, these would-be jihadists do not fit any particular ethnic, economic, educational, or social profile. The operations they mount, or attempt, range from shootings, to car bombs, to suicide attacks, to in-flight bombings of passenger aircraft.

We have seen a pattern of increasing terrorist recruitment of American citizens. In 2009, there were two actual terrorist attacks on our soil. You referenced the Fort Hood shooting, which claimed the lives of 13 people, and one U.S. military recruiter was killed, another wounded, in Little Rock, Arkansas. Many counterterrorism

experts talk about 2010 and name it the "year of the homegrown terrorist." Self-radicalization is an alarming development.

Our group issued a report, as you have mentioned, last fall on radicalization, and we are going to follow up this spring with a set of recommendations for dealing with this important and very sensitive problem.

We also face new threats, like the discovery in October 2010 of explosives packed in toner cartridges, addressed to synagogues in Chicago, and shipped on FedEx and UPS cargo flights from Yemen.

The cyber threat is also increasingly severe and poses a real danger to our critical infrastructure. Defending the United States against such attacks must be an urgent priority.

So we would like to offer our assessment today of where the government is in implementing 9/11 Commission recommendations.

On emergency preparedness, we have made some progress toward establishing a unity of command—in other words, one person responsible for coordinating efforts in a disaster. But having said that, our recommendations are still a long way from being fully implemented. We have found too many community leaders and first responders who have mentioned to us that many metropolitan areas still have not solved the problem of having a unified command structure. Moreover, it is unacceptable that the government still has not allocated the additional 10 megahertz of radio spectrum, the D Block that you mentioned, to public safety so that our first responders can communicate with each other in a disaster.

Now, I recognize the efforts and the leadership that you have shown through your bill. I believe the President supports such a recommendation, and Congress needs to act.

There have been improvements in transportation security, but technology still lags in screening passengers for weapons concealed in their bodies and for detecting explosives contained in bags. The GAO continues to find holes in virtually every single security layer that we establish.

Border security remains a top national security priority as terrorists continue to exploit our border vulnerabilities to gain entry into the United States. Several attempted attacks over the past 2 years were perpetrated by terrorists who could have been detected by the U.S. immigration system. We require a more streamlined terrorist watchlisting capability and better sharing of information between intelligence agencies and immigration authorities.

One area of progress is the deployment of the biometric entry system known as US-VISIT. We still lack, however, any comprehensive exit system. We do not know, in other words, when people leave the country. The Commission recommends that the government standardize secure identification and the Federal Government should set standards for the issuance of birth certificates and driver's licenses.

The REAL ID Act established these standards by statute. About one-third of the States have complied with this first-tier benchmark. The deadlines for compliance have been pushed back now twice. Delay in compliance creates real vulnerability and makes us less safe. We would ask that no further delays should be authorized.

Now I will ask my friend and partner, a man I admire as much as anybody in this country, Lee Hamilton, to continue.

TESTIMONY OF HON. LEE H. HAMILTON,[1] FORMER VICE CHAIRMAN OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Mr. HAMILTON. Thank you, Mr. Kean. Good morning.

I want to begin simply by endorsing what Mr. Kean has said with regard to the leadership not only of this Committee but specifically of the three Senators in front of me. I can remember coming to your offices shortly after the 9/11 Commission report was made. Mr. Kean and I spoke to each one of you. You were very courteous and receptive. But beyond that, you acted with genuine political leadership, and the country is very grateful to you.

I think there are a lot of reasons why the 9/11 Commission had a favorable response, but two of them: First, the families who gave sustained, sophisticated support for our recommendations; second, specifically the political leadership embodied by the three of you was just really quite extraordinary. And Mr. Kean and I are very grateful to you for what you have done. And when the Chairman a moment ago outlined your continuing hearings and investigations, I was immensely pleased to hear that because I think having been on the inside and on the outside, you have powers that we do not have in terms of getting people before you to provide tough oversight, and that continuing effort by this Committee is just hugely important because, as we will say often this morning, so much more needs to be done.

With respect to intelligence reform, the DNI has made progress in several areas: Increased information sharing, improved cooperation among agencies and of the analysis of intelligence, and sharpened collection priorities. Genuine progress, no doubt about it. Still, it is not clear to us that the DNI is the driving force for intelligence community integration that the Commission envisioned.

Some ambiguity probably remains with respect to the DNI's authority over budget and personnel, although that can be disputed, I guess. Strengthening the DNI's position would advance the unity of intelligence effort that we think is still very much needed.

I do not anticipate new legislation—you would know more about that than I on this subject—in the very near future. So we have to live with the statute that we have for an extended period of time. It may very well be that in the future some legislation could fortify the office.

Repeated indication from the President that the DNI is the unequivocal leader of the intelligence community, I think, would be greatly helpful.

The FBI has gone through dramatic change. I think it is moving in a positive direction, but in some sense incomplete. It has had, I believe, very strong leadership from Director Robert Mueller. It shifted resources to collect and analyze intelligence to prevent terrorism. That is an enormous cultural change, as you all know,

[1] The joint prepared statement of Mr. Kean and Mr. Hamilton appears in the Appendix on page 364.

away from its former focus strictly on law enforcement. Its progress has been significant but uneven.

The Fort Hood shootings highlight the lingering problems. Your report, which I have looked over quickly, has spelled that out, I think, in a very persuasive and compelling way.

Analysts do not appear to be driving intelligence within the FBI, nor have they achieved status on a par with the special agents who traditionally rise to management of the Bureau.

FBI headquarters components did not play a direct role in analyzing the threat posed by the person who later allegedly did the shootings. There were miscommunications, as Senator Collins has indicated in her opening statement, between the field offices, so the shift taking place within the FBI is still very much a work in progress. Congress needs to continue to help the FBI with its difficult transformation.

The CIA has improved its intelligence analysis and removed barriers between its analysts and operations officers. Our sense is that there has been more talk than action with respect to improvement in the CIA's human operations.

Acquiring well-placed sources is very difficult business, particularly in closed societies and among close-knit terrorist cells. More money and more personnel do not necessarily result in better agents.

While the CIA has attempted to recruit officers qualified in the languages of the greatest interest, that, too, is very hard. Part of the problem is that young people in our country, with some exceptions, of course, do not gain proficiency in foreign languages. Congress can help on that.

The CIA then must continue to rebuild. It will require strong support from Congress and the Executive Branch. We want the Agency to take calculated risks to protect the country. Congressional oversight must be depoliticized so that when the Agency fails, as it occasionally will, it is not inappropriately blamed for taking the necessary risks.

Improving information sharing across the Federal Government and with State and local authorities was a major recommendation. In some ways, I think the government is doing better. The Joint Terrorism Task Forces and Fusion Centers across the country have certainly improved information sharing. The National Counterterrorism Center has analysts and other officers from all agencies of the intelligence community working side by side and sharing information with their home organizations.

There have been some failures, as has already been indicated. There is no question that WikiLeaks' unauthorized publication of sensitive government documents has raised some genuine and real concerns. Those are legitimate. But the need to share information we think still remains highly important, and we should not backslide on that.

Congress has to help the government strike the right balance between the need to protect unauthorized disclosures and the need to share information to defend ourselves against the threats we face.

Among our major disappointments has been that the Administration has not empaneled the Privacy and Civil Liberties Oversight

Board. This was a major recommendation very strongly supported by all the Commissioners.

I am informed—I am not sure I am quite up to date on this—that the Administration has nominated two individuals for the panel. I know one of them personally. As far as we know, they have not yet been confirmed, and the panel certainly has not met. The Administration, I believe, needs to push this on a priority basis because that board has a lot to do, and I think this Committee can be helpful in pushing the Administration.

We are equally disappointed that Congress has not reformed itself along the lines we recommended. We recommended that Congress create a Joint Committee on Intelligence or create House and Senate committees with combined authorizing and appropriation powers. Those recommendations may be a bridge too far.

Last week, the Chairman of the House Intelligence Committee announced a decision to include three members of the House Appropriations Committee to participate in House Intelligence Committee hearings and briefings. That appears to us to be a positive step, but obviously there is more to do.

Oversight of the Department of Homeland Security is fractured. That massive Department will be better integrated if there is better integrated oversight. I know the concerns you have expressed about that. It is in our country's security interest that Congress make committee reform a priority.

Preventing the spread of nuclear weapons must be a national priority. The Administration hosted a major nonproliferation summit last year and announced a new initiative to secure all nuclear materials by 2013. It plans to spend $14.2 billion over the next 5 years to secure nuclear and radiological materials.

May I say outside my statement that because of other responsibilities I have dealing with nuclear power, I have recently had the occasion to listen to some highly qualified people within our government, and I believe the access to nuclear materials and the ability to use those materials and to explode them is much greater than people generally think. And so I hope the Congress will keep a hard, sharp focus on this question of nuclear proliferation. I know there are some suggestions to cut some of these important programs. Money is not everything here, but we must not weaken or underfund what President Bush and President Obama have both said is the highest priority security need.

Now, at the outset of his Administration, President Obama issued Executive Orders that brought the United States into line with international norms for the treatment of detainees. That fulfilled part of our recommendation. We believe there is a conflict between the rule of law and holding detainees indefinitely without resolving their cases. Both Presidents Bush and Obama have really wrestled with this problem. It is a tough one. President Obama took a step forward by requiring periodic reviews of the status of detainees, but there is an awful lot more to do. The Congress and the Executive Branch simply have to agree on a statutory base to give us a comprehensive approach to dealing with the detainees.

Congress and the Executive Branch need to agree on the rules of evidence and the procedures that should be applied in determining how to deal with these detainees. I do not think this is a

problem that can just simply go on and on and on. You need a statutory basis—and I do not suggest it is easy to reach it—on how to deal with these potentially very dangerous detainees.

We had a number of foreign policy recommendations in the report. Events today in the Middle East and North Africa clearly indicate that the region is in a state of upheaval, and it is quite unclear to any of us how it will emerge.

We addressed the role that U.S. foreign policy plays in counterterrorism, but we did it, to be honest about it, with considerable modesty. We believe that although the countries share a common religion, their people have many cultural, national, ethnic, and tribal differences, and therefore, we have to deal with them on a country-by-country basis. We want our country always to advance its core values, but a pragmatic approach for each country, one that supports an agenda of opportunity for the Islamic world, we think is necessary.

So, to conclude, significant progress has been made since 9/11, and our country is undoubtedly more secure. Yet important 9/11 Commission recommendations remain to be implemented, and over the next few years, a lot of heavy lifting still needs to be done.

As Mr. Kean mentioned just a moment ago, the fact that we have not resolved this radio spectrum problem and have not resolved the unity of command is just really distressing to us. Those are two no-brainers with regard to the safety and security of the country. Some progress has been made in both areas, but not nearly enough.

Congress has resisted reorganizing its own institutions, and streamlining congressional oversight of the intelligence community and the Department of Homeland Security would go far toward advancing unity of effort in the intelligence community and within DHS.

Also the DNI needs a clear-eyed appraisal. I think it is functioning reasonably well. Likewise the FBI. We have concerns about each, and our goal really should be to strengthen both the DNI and the FBI.

The terrorist threat will be with us far into the future, demanding that we be ever vigilant. Our national security departments require strong leadership and attentive management at every level to ensure that all parts are working well together and that there is innovation and imagination. Our agencies and their dedicated workforces have gone through much change, and we commend them for their achievements in protecting the American people. But there is a tendency toward inertia in all bureaucracies, and vigorous congressional oversight is just imperative to ensure that they remain vigilant and continue to pursue needed reforms.

So our task is challenging and difficult. We constantly have to assess our vulnerabilities and anticipate new and evolving lines of attack. We have done a lot. We can look back with some satisfaction, but there is an awful lot more to do.

We are very grateful to you for the opportunity to testify before this Committee, which has provided longstanding leadership on these issues, and we will do our best now to respond to your questions.

Chairman LIEBERMAN. Thank you both for those thoughtful opening statements. I think you really helped us get some perspective on where we have come in the last several years, certainly since 2004, when the 9/11 Commission Act was enacted. But you have also given us a clear statement of unfinished business and priorities for the future, and I appreciate that.

Before I begin my questioning, I want to note the presence since we began of Abraham Scott, whose wife, Janice, died at the Pentagon on 9/11, and he is another one of those family members who have continued in the battle to do everything they can to make sure nothing like this happens again.

I thought both of you summarized well where we have come and also noted that the steps we have taken to improve our homeland security, including those very significant steps that were part of your recommendations that we adopted, have strengthened our security, but that the nature of the threat has changed. We can never say never, but certainly our defenses against a sophisticated 9/11-type attack are way up and, therefore, the prospects of that happening are down, thank God.

There is a high risk right now of smaller attacks than 9/11, particularly of attacks that come from within the country because that has become a focus of al-Qaeda and all the other international Islamist terrorist groups.

I wanted to begin by asking you, Governor Kean, just to talk a little bit more about the inadequacy of unity of command at this point and what you think we can do about it.

Mr. KEAN. Well, this was one of the real problems on 9/11. Who was in charge?

Chairman LIEBERMAN. Right.

Mr. KEAN. And so our recommendation very strongly to all communities has been there has to be one leader. Now, New York City made a lot of progress in that regard by putting everything under the police department. Some cities have followed that pattern and some have not, and so there are still a number of communities, some of them fairly sizable, where people tell us there is still that question. If something really happens, who is in charge?

Businesses have made more progress. I think almost all major businesses I know now have somebody who is in charge if something happens. They know what they should do. They know where employees ought to go. All that is in place in a lot of major businesses. But in communities, not as yet, and we think it is a very serious problem and one that we have to address and make it, as best we can, a requirement that somebody be in charge.

Chairman LIEBERMAN. Well, I am really interested that you have focused on the local or metropolitan level, and I think we have to do some thinking about that to see whether we cannot create some requirement or incentive to bring about that unity of command at the local level, perhaps by making it a condition of some of the homeland security or other grants.

Let me take you to the national level. I am reading from Section 13.1 of the Commission's report on Unity of Effort Across the Foreign-Domestic Divide, and this section of the report notes specifically that during the Commission's hearings, members of the Commission often asked, "Who is the quarterback? The other players

are in their positions doing their jobs. But who is calling the play that assigns the roles to help them execute as a team?"

To respond to this need, in my interpretation of the Commission's report, you recommended creating a National Counterterrorism Center with the responsibility to develop counterterrorism plans that integrate all the instruments of national power, and that was, I think, one of the most significant recommendations and one of the most significant components of our legislation.

So as you look back nationally now, are you satisfied there is clarity and unity of command at the national level and that we now have a quarterback? And is it the National Counterterrorism Center?

Mr. KEAN. Well, it is the National Counterterrorism Center and, of course, the DNI.

Chairman LIEBERMAN. Right.

Mr. KEAN. In combination. They are the quarterback. Now, whether they are being implemented as the quarterback, whether or not they really have the power that you intended when you wrote the law and that we intended when we made recommendations, I do not know.

Chairman LIEBERMAN. Yes.

Mr. KEAN. Because the signals sometimes are mixed. And we have to have unity of effort in that regard. We have to have the quarterback. And I would suggest that you would probe that area and find out whether or not the quarterback is in place and whether or not the quarterback has the powers that you intended him to have in the legislation.

Chairman LIEBERMAN. There is no question that the National Counterterrorism Center has created unprecedented cooperation between components of our security and intelligence communities. In that sense, the dots are all on the same board now. One of the problems, I say in passing, that we have noted in some of our earlier hearings and it was a cause of some of the cases that we have studied that were not as we would want is that the problem now is there are so many dots on the same board that it is hard in real time to separate them out to connect the ones that ought to be connected, but they are not on separate boards anymore.

Mr. HAMILTON. Mr. Chairman, may I say a word about it?

Chairman LIEBERMAN. Yes, please.

Mr. HAMILTON. You have two problems there. You have raised both of them. One is the scene of the disaster.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. And there it is kind of a no-brainer, too, for me anyway, that someone has to be in charge. Now, that creates difficult political problems because the governor wants to be in charge, the mayor wants to be in charge, county officials want to be in charge. And that is the reason it has not been resolved because the politicians are unwilling to address the question because it is a tough one to say who is in charge.

Now, I do not know whether that barrier can be overcome or not, but in terms of saving lives, it is an easy question to answer. You have to have one person making decisions with regard to sanitation, public health, food, housing, and transportation.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. They have to make thousands of decisions within a matter of a few hours, really, at these scenes. And if you have confusion of command at that locale, you lose additional lives.

So that is why we think it is an important matter. I really do not know how well different metropolitan areas around the country have addressed this problem, but I am very uneasy about it, and I do not really think it has been solved in most areas.

Now, the second problem relates to a unity of effort in the Administration, which is the broader question.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. Who is the quarterback? I follow this reasonably carefully. I do not pretend to know everything about it. I do not know who the quarterback is. And I will give you my impression. My impression is that the number one official within the White House is John Brennan on these matters. That makes me a little uneasy—not because of him. He is an extremely dedicated, important, capable man. But he is right in the center of the policy world at the White House. He is not removed from it like I generally want intelligence officials to be. And so I am not sure whether he is the right person to do it. But if he is, then it seems to me there ought to be a very clear designation that he is in charge of homeland security and counterterrorism.

Today, quite frankly, from where I sit, it looks to me like a number of different people are involved in it, including Mr. Brennan, including the Director of National Intelligence, including the DHS Secretary and several others. I do not know who the quarterback is, and I can identify the Commissioners who raised that question all the time in the meetings we had, Mr. Kean.

Mr. KEAN. That is right.

Mr. HAMILTON. My guess is those same Commissioners would be raising the same question today, who is the quarterback?

Chairman LIEBERMAN. That is very helpful commentary, and I agree with you that we have the combination—and I am simplifying here—of the critical role of intelligence in counterterrorism and homeland security, but also then the other roles, which are different, of preparedness and prevention and response. And I agree with you, Mr. Hamilton, that the top person today in our government is John Brennan, the Deputy National Security Adviser for Homeland Security and Counterterrorism. And, again, I have great respect for his ability, etc. Whether that is the right place for that role to be is an important question.

Mr. HAMILTON. The President should have the right to organize his White House he wants to organize it.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. And maybe the President is comfortable with this.

Chairman LIEBERMAN. Yes.

Mr. HAMILTON. As an outsider here, who looks at it fairly carefully, it is not clear to me that the lines of authority are precise.

Chairman LIEBERMAN. Yes, and I think you have quite accurately identified the key players. It is the Secretary of Homeland Security, the Director of National Intelligence, the Director of the National Counterterrorism Center. And, of course, there are others—the FBI Director——

Mr. HAMILTON. Yes.

Chairman LIEBERMAN. But more than anyone else, Mr. Brennan seems to us day to day to be coordinating that effort. There are different roles here, although you could pick one of those other players and make that person the coordinator. It might be the Secretary of Homeland Security who has both operating and intelligence authority. You have given us a good charge for our review during this year.

My time is up. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Let me pick up on this very issue of who is in charge. To me, it was very clear when we passed the Reform Act in 2004 that we wanted the DNI to be in charge. That is why we created this new quarterback position. And yet I completely agree with Congressman Hamilton that in this particular Administration, the person who is in charge is Mr. Brennan at the White House. And putting aside his enormous capabilities, which we all agree to, the problem with that situation is there is no accountability to Congress. It is a member of the President's staff, so we cannot call Mr. Brennan to testify before us. We cannot hold him accountable for decisions. And I think that is another very big problem.

The other area of confusion of command, as Congressman Hamilton has said and Governor Kean well knows, is when a disaster strikes or there is a crisis situation. And we saw this with Abdulmutallab where there was tremendous confusion over who was in charge and who should make decisions. In that case, it ended up being the Attorney General who made the decision on how to treat Abdulmutallab without any consultation whatsoever with the DNI, the Director of the National Counterterrorism Center, the Secretary of Homeland Security, or any top intelligence official on whether or not Abdulmutallab should be questioned about whether there were further plots, and that was a lost intelligence opportunity.

Are these problems that we can fix through legislation? Or are they problems that depend on an individual President setting up who is truly going to be in power?

The reason I ask this question is when I go back and review the language creating the DNI, it is pretty strong language. Now, we tried to get it to be even stronger in the area of personnel, but in fact, the DNI has strong authority to set priorities for the intelligence community, to oversee the budget formulation, to make some personnel decisions.

Is this really a case where we need to strengthen the law? Or is it a case where the President needs to empower the person we intended to be empowered? I would like to hear from both of you in either order on this question.

Mr. HAMILTON. I think the latter—the President has to step in here. Now, any law, as we all know, can be strengthened. But as I suggested, this law is not going to be changed in the immediate future. It took you several years to get it on the statute books, so maybe in the future it will be clarified. But, Senator Collins, I basically agree with your comment that there is sufficient authority in present law. We envisioned, of course, that the DNI would be the

central powerful driver of the intelligence community. I do not think he has been.

Now, I want to say here, too, you know I have known all of these men that have held that position. It is a very tough position. We have had very good men in that position. They really have been quite strong. But that line of authority is not as clear as it should be, and so I think given the circumstances that you now have, your second choice, that is, the President has to step in and make it very clear with regard to his authority in the intelligence community, over budget and over personnel and over transfer of funds within the budget. And so far as I can see, that really has not been done.

Now, having said that, the DNI deals with some pretty powerful players—the Secretary of Defense, the CIA Director—and if they get a decision within the bureaucracy they do not like, they will go directly to the President. Fair enough. So the DNI may have authority and he may try to exercise it, but he has to exercise that authority with extraordinary skill and discretion. And these are all major players within the Administration, and so that power has to be very skillfully exercised.

But I personally think the system is going to work a lot better if you have someone at the top of it who is the driving force, who is recognized as the center of power, who has the authority, and obviously has to have the support of the President, to do the things that need to be done to get unity of effort.

Senator COLLINS. Thank you. Governor Kean.

Mr. KEAN. Yes, I remember when the bill was going through. It was weakened a bit in the House, and I remember talking to Mr. Hamilton about it at the time, and he said, "Do not worry because in the end it is the President. And if the President gives the DNI the authority, the DNI will be just the way you want it to be. If not, the law is not going to help." And that is where we are.

My own belief is the law says the DNI ought to be the top intelligence operative, I think it will work better that way, and that is probably how it ought to be. But if this President wants somebody else, then my only recommendation would be that he make that clear and that both publicly and within the Administration everybody knows where the lines of authority are, and if somebody else is going to be in full charge, let us say who that person is, and then everybody knows, because the worst thing of all is a vacuum or confusion or lines that are not clear. The President is the only one who can make those lines clear, and the President is the only one who could make it happen.

Senator COLLINS. I agree that the President's response is absolutely clear and needs to be clearer here, and that if the President does not empower the DNI, we can write all the language in the world, and the DNI is not going to truly be in charge. But I also remain very concerned about the lack of accountability to Congress and the public when it is a member of the President's staff who is running the intelligence community.

Mr. HAMILTON. I just want to support what you said. I think that is terribly important.

Mr. KEAN. Very important.

Mr. HAMILTON. The person who is in charge, whoever it is, ought to be accountable to Congress at all times. That is just fundamental, it seems to me, to the way this place ought to operate.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks very much, Senator Collins. Of course, I agree with you, and it strikes me that ultimately the DNI has ample authority—not as much as any of us wanted, but ample authority in the current statute, but it really requires the President to make clear that the DNI is the person in charge of the intelligence community.

We all expected that coming in as a new position to oversee existing agencies, which have a real life of their own and a constituency of their own, would be difficult. And it is interesting that General James Clapper—really to just amplify a bit on what I said in my opening statement—I think because of his background in the military and credibility at the Pentagon, has actually negotiated an agreement with Secretary Robert Gates, which will enable the DNI to have much more authority with regard to intelligence budgeting, appropriations, than was the case at the beginning of the office, and that is good.

The question of who is on top overall in the counterterrorism effort is a complicated one because there is not only the intelligence community but all the others—the operators, the preventers, and the responders. But I, again, agree that it has to be somebody at the top—nothing negative about Mr. Brennan—who is accountable to Congress and the public. And we have to think about how to deal with that problem.

Mr. KEAN. Yes, I think that is very important. When we first talked about the position, I think what we envisioned was a man or woman who would step into that position and stay 5 or 6 years and develop the position, strengthen it and all of that. We have had this rotating door, really, of very good people, but in and out.

Chairman LIEBERMAN. Right.

Mr. KEAN. And that has been one of the problems with the DNI, and hopefully we have one now who will stay for a while.

Chairman LIEBERMAN. I hope. Thank you. Next in order of arrival, Senator Akaka and then Senator Carper.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, for holding this hearing, and I would like to welcome Governor Kean and Congressman Hamilton, and thank you for being here today.

Although many of the information-sharing and intelligence shortfalls that the 9/11 Commission identified have been addressed, critical work remains to ensure that we have an agile and well-coordinated response to terrorist threats, and you have been discussing this. Supporting our Federal workers at DHS, the intelligence community, and other agencies who make daily sacrifices to keep us safe is essential to this effort. Additionally, we must never lose sight of the privacy and civil liberties implications of our efforts to protect the Nation. In particular, I agree with our witnesses' comments that the Privacy and Civil Liberties Oversight Board must be set up immediately.

Congressman Hamilton, as you know, I believe that GAO could assist our efforts to strengthen oversight of the intelligence community. In response to my question in 2007, you stated that GAO should have the same authorities within the intelligence community as it has in other agencies. Key principles of my Intelligence Community Audit Act were included in the Intelligence Authorization Act last year. Under this legislation, the Director of National Intelligence must issue a directive to facilitate GAO audits and evaluations of the intelligence community.

What elements should be included in the DNI directive to promote effective oversight?

Mr. HAMILTON. Senator, I am not sure I understand the question. What elements should the DNI insist upon for oversight?

Senator AKAKA. To include in the directive to promote effective oversight.

Mr. HAMILTON. The DNI's oversight of the intelligence community or congressional oversight?

Senator AKAKA. Well, either one.

Mr. HAMILTON. Well, I am not sure I have the thrust of the question in mind, but I am deeply impressed that only you folks in the Congress can effectively oversee the intelligence community. The press does not know what is going on. Those of us outside Congress do not have the information that you have and your staffs have about what is going on. So unlike most other areas of our government, the only really effective independent oversight of the intelligence community can come from the Congress.

Now, you have the President's Intelligence Advisory Board. I serve on that. But they are all appointed by the President, and they are not really an independent group. So in all of the recommendations we made, we thought that the strengthening and persistence of congressional oversight was just absolutely critical to the success of the implementation of the recommendations.

Now, I know that there is a lot of internal oversight that takes place within each agency, and I think within the DNI's office as well, and that can be important to oversee it. But that is not an independent oversight. That can only come from Congress. I support giving the GAO ample powers to review the intelligence community, and I agree with you, Senator Akaka, that GAO should have a key role. The DNI should issue directives to intelligence agencies requiring their cooperation with GAO.

I do want to pick up on your observations about the Privacy and Civil Liberties Oversight Board because this has been a source of enormous frustration to Mr. Kean and to me. I just cannot figure it out. I do not know what President Bush and President Obama think. They just have not put an effective board in place, and I cannot understand why.

Now, this is urgently needed because in homeland security and intelligence matters, you have greatly accelerated surveillance. All kinds of provisions are written into the law that expand the powers of the FBI and the intelligence agencies, understandably in most cases, I think, to check on what the American people are doing. And I think somebody needs to be out there to keep their eye on these folks in a very aggressive way because the security people

within an agency almost always win the arguments, and you need an independent source to really keep your eye on them.

So we favored a strong, robust oversight of civil liberties and privacy with the power to issue subpoenas and a power to call people in front of them and keep a watchful eye because I think there has not been enough attention to the question of civil liberties and privacy in general with regard to homeland security.

Mr. KEAN. I might just add that Mr. Hamilton is right. Nothing has frustrated me more, of almost all our recommendations, than the lack of progress on civil liberties and the board, and I do not know what problems the administrations have with the bill that you passed. But if there is a problem with it, if there is something wrong with the structure, if they think it is intrusive or something, then tell us and maybe you will change it. But to not appoint members and to be almost 2 years into an administration which has not even nominated enough members to make a quorum is frustrating and makes no sense to me and leaves a big hole in what we should be doing.

So again, I do not understand it. I am frustrated by it. But if there is a problem, I wish they would tell us what the problem is.

Senator AKAKA. Thank you for those observations. I really agree with you that we need to set that up immediately.

Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka. Senator Collins and I were talking. We can address a letter to the White House to ask what is going on here because I do not think there is any policy or ideological opposition to the board. I suppose it is always possible that there are elements within the intelligence community that do not like the idea, but I actually have not heard that either. I think we will address a letter right away and see if we can get you a response.[1]

Mr. HAMILTON. Thank you.

Mr. KEAN. Thank you very much.

Chairman LIEBERMAN. Next is Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman.

Mr. Chairman, we have gathered before us today two of my very favorite people in public life: Mr. Kean, a great governor of New Jersey, our neighbor across the Delaware River, and someone for whom we have huge respect in our State; and Mr. Hamilton with whom I was privileged to serve for 10 years. I was privileged to think of him as one of my mentors. And it is just great to see both of you still so active, vibrant, and contributing on so many different levels.

About once a month I am asked what is wrong in Washington, and one of the things I always talk about is the lack of trust—sometimes a lack of trust between parties, sometimes a lack of trust between the Executive and Legislative branches, sometimes a lack of trust between Committee chairs and ranking members, and this Committee is an example of what you can get done when

[1] The letter referenced by Chairman Lieberman appears in the Appendix on page 387.

you have a trusting relationship, with Senators Lieberman and Collins.

Every month I talk about the trust that the two of you developed when you assumed your positions as the leaders of the 9/11 Commission and how you provided an example through that trust to the other members of the Commission and achieved extraordinary consensus and came to us and enabled us, with your leadership, to reflect and to follow that example. So I just wanted to lead off by saying that.

I am fortunate to chair a subcommittee of this Committee. It has a long name, but it is called Federal Financial Management for short. We poke in almost every nook and cranny of the Federal Government to see if there are ways that we can get better results for less money.

In this hearing room yesterday, we heard from, among others, the Department of Defense and GAO, and we were looking at the GAO report that came out yesterday that cited major weapon systems cost overruns for 2010 of $402 billion, up from $42 billion a decade earlier. In this room, we have had hearings in the last month on improper payments—not fraud, but just mistakes, overpayments for the most part. We have a new number for improper payments for last year—$125 billion—not counting the Department of Defense, and not counting the Medicare prescription drug program.

We have had hearings on surplus property. We have thousands and thousands of pieces of surplus property we do not use, we need to get rid of, and they are just a burden on us, $300 billion, plus tax gap monies that are owed and not being collected. Those are the kinds of things we focus on in this room.

With that spirit of trying to change the culture around here or at the Department of Defense or in the Legislative or Executive Branch throughout the Federal Government, to move from what I call a culture of spendthrift to a culture of thrift, would you join with us today maybe just to think about it and then to come back to us in writing? I know there are things we are doing, entitlement programs, we have had many hearings on those as well, and domestic discretionary spending programs and defense programs, things that we are doing where we can get a better result for less money or a better result for not a lot more money. With that spirit in mind, can you just think out loud with us for a minute or two here today about if there is some way that we can get a better result in this area of national security and homeland security without spending more money or even spending a little bit less?

Mr. HAMILTON. Well, no, my impression, Senator, is in the area of homeland security and intelligence—I know this is not the Intelligence Committee—the whole question of cost effectiveness rarely arises.

Senator CARPER. That is true.

Mr. HAMILTON. We have been set on a course, for understandable reasons, since 9/11 to create enormous increases in intelligence budgets and a massive new Department, DHS, and everybody has hit the full-speed-ahead button. I do not have the specific figures, but you have had an enormous increase in the total amount of

money spent in intelligence just in the last few years, for reasons we all understand.

So when you began your comments on cost effectiveness, getting better results for less money, my response was, "Bravo," because I think you need a hard-headed business attitude, if you would, in this area, which has been totally absent for 10 years. There is probably a little exaggeration in what I have just said, but I think cost effectiveness here would be important and making these fellows come in who head these agencies and not only hold their feet to the fire with regard to homeland security and stopping terrorist attacks, but making sure this money is being wisely spent. It makes a lot of sense to me. So I think you perform an enormously important service as you push the whole business of cost effectiveness.

Senator CARPER. All right.

Mr. KEAN. I think there is no question, whether it is public or private sector, if you ramp up as fast as we felt we had to ramp up after 9/11, you are going to have problems. You are going to overspend. You are going to waste some money. And I am sure that has been done. Spending on non-military intelligence, that number is now public. I guess the military intelligence spending is not public yet. I assume, combined, we are somewhere around $80 billion, I would guess. And that is a lot of money, and a lot of it ramped up in a great hurry. So I think what you are doing is very important. We need not only to do this well, we need to do it efficiently.

Senator CARPER. If I could, I am just going to ask you two to think about this for a while and maybe respond on the record after you have given it some more thought.

One last question, if I may, Mr. Chairman.

Chairman LIEBERMAN. Please.

Senator CARPER. Going back to the early 1990s, we have seen a couple of countries come back and forth across our radar screen. They include Somalia and Yemen. Both countries have been in almost perpetual decline for, it seems like, a couple of decades. And as a result, we have seen two very different dangerous groups that are proving a clear and present danger to our country. They are al-Shabaab from Somalia and al-Qaeda from the Arabian Peninsula operating in Yemen. Both have been directly and indirectly responsible for the December 25th Christmas Day bombing attempt, the Fort Hood attacks, and Alabama and Minnesota terrorism cells. And it is clear that if these two countries implode, they will not only pose a more severe threat to us, but maybe to the rest of the world.

Could either of you please describe your thoughts on the threat that these groups pose to the United States and if our Federal Government is doing enough to prevent these two specific terrorist groups from growing into a more powerful global entity?

Mr. KEAN. You are right. It is interesting how this business has evolved. Years ago, we used to worry about urban areas and powerful countries and so on. Those were the threat. Now it is the ungoverned areas of the world. It is the wild areas. It is the areas where there does not seem to be any kind of legitimate authority where these organizations develop. And I think beyond even Yemen and Somalia, we do not know what is happening now in that area of the world in some other countries. We do not know what is going

to happen if and when Gaddafi falls and how tribal that will become. We do not know what is going to happen in some of these other areas that may or may not disintegrate into these kind of areas.

So this has to continue to be our priority, and with the government of Yemen collapsing, it is going to be worse before it gets better. I know we are not doing enough—I know we are concentrating on it. I know the intelligence communities are working hard to learn what they can learn. We still do not have enough people, enough boots on the ground, the boots of intelligence people on the ground in those areas. We are depending on other intelligence agencies in that part of the world, which now may not be able to give us that information anymore because of what has gone on with their governments.

So it is a continuing and very serious problem, and we have to be ready to address not only those two areas, but other areas that may develop.

Senator CARPER. Thank you. Congressman Hamilton.

Mr. HAMILTON. Well, I think you have put your finger on maybe the most difficult problem with regard to protecting ourselves from threats from abroad. You have governments in these countries that really do not govern throughout the country. You have all kinds of tribal, ethnic differences. It is a very hard problem.

I think we have to work as a Nation on developing the capabilities to deal with these countries, and I must say I am not quite sure how I would spell out those capabilities. Supporting the government is often done to try to ensure stability, but we have surely seen the limits of that in recent years.

So I think we just have to develop the expertise for these countries and figure out on an ad hoc basis with each one of them what kind of capabilities exist within the country to counter the extremist groups. If you have a government that is reasonably stable, reasonably competent, then you have to work with that government for sure. And if you do not have a stable, competent government, then we may have to insert capabilities ourselves. You cannot generalize here too much. But the kind of plots we had that went with the FedEx and UPS packages that were sent into the United States that originated, I think, in Yemen indicate to us the challenges that we confront. You have to have a multi-layered approach, obviously, to deal with these threats, not just in-country but trying to stop it when it is in transport, whatever the threat may be.

We described in our report the evolving nature of the threat, and this is, among other things, exactly what we meant, and it is a formidable challenge for us.

Mr. KEAN. You cannot do it in a public hearing, but when you have your private hearings with members of the intelligence community, I would ask: Have our sources of information been compromised and how much? Where did we find out the information we have used to stop some plots? We received information from various governments. Was it the Egyptian government? And can we still depend on them for that information?

Did we get information out of even Libya? Which, obviously, we cannot count on anymore. A lot of those people who were working with us probably are not working with us or do not have the ability

to work with us today, and if we are losing those sources of information, what are we going to do about it?

Senator CARPER. Good. Thank you for those responses.

Mr. HAMILTON. I think the Afghanistan experience should tell us not to ignore these countries as difficult as it may be. So if we have intelligence that in Yemen or in Somalia there are groups that are plotting against the United States or our allies in some way, then I think we have to get our brains together and figure out the best way to do it. And depending on the strength of the intelligence, you may want to use drones; you may want to use special operation forces. Your preference would be to have the local government deal with it. But if the local government does not deal with it, then we have to take a position that it is a threat to our national security and we have to deal with it.

Senator CARPER. All right. Thank you for those comments.

Mr. Chairman, you have been very generous with the time.

Chairman LIEBERMAN. No, not at all.

Senator CARPER. I just want to say again to both of you, thanks so much for your continued leadership and for being an inspiration to us all.

Mr. KEAN. Thank you.

Chairman LIEBERMAN. Thanks, Senator Carper. Excellent questions.

Governor Kean and Congressman Hamilton, I have a few more questions myself.

We have talked about the evolving nature of the threat, and I know that we agree that one of the most significant developments in terms of the Islamist terrorist threat since 9/11 has been the homegrown radicalization and self-radicalization. It may have existed in some way before 9/11, but not really in an observable or consequential way, and we have seen it over and over again now in cases that have existed, including the two that you mentioned, Governor Kean, in 2009, in which successful terrorist attacks were carried out, both the Bledsoe case in Arkansas and the Hasan case at Fort Hood. Those were both homegrown, self-radicalization cases. In the case of Bledsoe, he did go to Yemen for a while. It is not totally clear who he connected with there, but he was radicalized here.

By coincidence, just this morning I was informed by my staff that last night the most recent edition of a magazine called "Inspire," the fifth edition, which is published by al-Qaeda in the Arabian Peninsula, appeared. It is quite remarkable, very slick, printed in English, published in English, so aimed at an English-speaking audience, including here in America. Perhaps we should take this as some kind of compliment, if you will, that we have built up our perimeter defenses, you might say, to protect the homeland such that our foreign enemies are now trying to develop within our country people who can carry out terrorist attacks.

Anyway, we have held a number of hearings and made some recommendations about this. It is a complicated problem because unlike 9/11, which we should have detected and stopped, very often these are people operating as so-called lone wolves. So I know that your National Security Preparedness Group has focused on this problem. I wanted first to thank you for that and say how much

I appreciate it. I know you have described the problem, and as you mentioned, there will be recommendations coming this spring. I just wanted to give you the opportunity to comment on this new, very significant threat element in our attempts to protect the homeland. I do not want you to pre-empt your recommendations, but is there anything you would like to say about what more you think the government ought to be doing to stop the problem.

Mr. KEAN. Well, it is extraordinarily difficult because as you say, our defenses, based on our recommendations in many cases and on your work, have been to stop people like the 9/11 co-conspirators from coming in from other countries and doing us harm. Those defenses are not adequate when the dangers come from somebody who is an American citizen, with an American driver's license, an American passport, and all of that. They are inspired, a lot of these people, from the Internet.

One of the missing pieces that we never quite nailed down in the 9/11 report was whether or not anybody in this country supported or helped the terrorists in any way, though we had a suspicion al-Awlaki might have. And we mentioned in our report that we lacked the staff and the time to really dig into it further, but he was very suspicious, as were his contacts. Well, he is now gone, of course, and has become one of the people who is recruiting from overseas. So he has a definite connection to even the 9/11 hijackers.

Chairman LIEBERMAN. Correct.

Mr. KEAN. So we think it is a terrible problem, a difficult problem, though we are not talking about a lot of people. We do not believe there is enormous radicalization taking place. It is a very small number of people. But these people, many of whom do not look like your traditional terrorists and have American passports, present the greatest danger right now, and we think there ought to be a real effort and a real dedication by our intelligence communities to implement a strategy to deal with it. And I am not sure that is in place as yet.

Mr. HAMILTON. Obviously it is a lot better to stop terrorist attacks before they happen and prevent people from being injured. Our group is working on a radicalization report, which we hope will have some recommendations for you before too many weeks go by.

Chairman LIEBERMAN. Good.

Mr. HAMILTON. Two or three things come to mind. One is, this is a good illustration of how important it is to work with State and local officials. In my own experience in my State, I have seen communities that have reached out to the Islamic community and those that do not. Community leadership makes a difference here, and that community leadership knows their community better than anybody else, and I think it is very important for Federal officials—and I know it is not easy because there are so many communities in the country—to strengthen their State and local contacts in order to better prevent radicalization.

Second, I think there has to be a clear outreach to the Islamic community leadership. I know there are some controversial aspects to this, but most of the Islamic leaders with whom I have had any contact want to help.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. And believe you me, they know their communities—not perfectly but pretty well. And so good liaison with those people is very important.

We have a representative today from the NYPD, and he would know much more about this than I, but I am impressed with the way the NYPD has contacted various communities within the New York City region and has reached out to try to understand those communities better.

Look, the people who cause you trouble are young men, for the most part, so they are the keys for you. Now, maybe not exclusively but for the most part. And the community leadership has to understand their own young people in a sense. And I think the NYPD has set an example of contacts that other metropolitan areas could follow.

The other thing we talked about earlier, I guess, is the coordination of the effort within the Federal Government. If you ask the question today who is in charge of dealing with homeland radicalization in our government, I do not think I could answer that. Maybe someone from the government can, but it is not very clear to me who it is. But there ought to be somebody in charge.

Chairman LIEBERMAN. I agree. We have asked that question, and the answer we received was that the Director of the National Counterterrorism Center is in charge. But that surprised us, frankly, and there is an attempt to try to organize this better and a recognition that this is a real problem. But we will benefit from your recommendations greatly, and I look forward to them.

Mr. HAMILTON. Well, they need operational responsibility.

Chairman LIEBERMAN. That is the problem, and interestingly enough—and this now goes back a while, maybe 2 years ago, so it is somewhat dated—we had a hearing with some leaders of the Muslim-American community, and we asked, Is there any agency of the Federal Government that has done outreach to your community or which has done the most? And to me the surprising answer we received was, yes, the FBI through its State offices had been reaching out quite a lot and had some communication.

But, Mr. Hamilton, the NYPD sets the standard here. This is not inexpensive. It is labor intensive. Maybe because they were so traumatized by 9/11, they have committed a lot of resources, and they have excellent communications with the Muslim-American community. I think the LAPD does a good job, too, but then there are some places in the country with significant Muslim-American communities where my impression is that the outreach and communication from local law enforcement is slim to none, and that is a dangerous situation. So we look forward to your recommendations on that.

Senator Collins mentioned something at the beginning, and I am just going to do it quickly because I know we are both concerned about this, and this is to come back to your report. You did a great service by identifying the enemy here and saying, yes, it was al-Qaeda. But more broadly, it is an ideology, which is violent Islamist extremism. That is what inspired the attacks of 9/11 and has continued to inspire this myriad of attacks large and small since then. And I thought you made a substantial contribution when you said, "We are not fighting terrorism, some generic evil."

We are fighting an ideology, if you will, a corruption of a theology. You also said, "Our strategy must match our means to two ends: Dismantling the al-Qaeda network and prevailing in the longer term over the ideology that gives rise to Islamist terrorism." That is a direct quote from your report. Talk about frustration. We have been so frustrated that the Administration continues to resist identifying the ideology, preferring instead to say that we are in a conflict with violent extremism. Well, it is violent extremism, but it is a particular kind of extremism.

In our report on the Fort Hood attack by Hasan, we pointed out that the Defense Department has even tried at one point to characterize the threat represented by the Fort Hood attack as workplace violence. But, of course, it was a lot more than that.

So, I guess I understand what is going on here. Somebody thinks that if we use the term "Islamist extremism" it is offensive to Muslims. But I think it is quite the opposite because we are talking about, as you said, Mr. Kean, a very small group within a larger community, certainly here in America, of people who are followers of Islam, not Islamist extremism.

Anyway, I invite a response to this continuing problem.

Mr. KEAN. Well, we worked on that one. We worked on how to characterize it. We had debates on the Commission about it, and we did research.

Chairman LIEBERMAN. Right.

Mr. KEAN. For instance, some people suggested "jihadist." Well, jihadist has some good connotations, too, in the Muslim world.

Chairman LIEBERMAN. Right.

Mr. KEAN. And so we rejected a lot of these terms. "Islamist" does not, and Islamist extremism is what it is. And I think words are important and language is important, and I think naming the enemy is important. And Islamist extremism is as good a term as we have been able to find for actually identifying what the problem is and who the people are. And I think everything from our research shows that the community itself accepts that term.

Chairman LIEBERMAN. I appreciate that answer. I have continued to use the term that you used because "Islamist" makes the point that a political ideology has exploited a religion. It is not Islam.

Let me ask the last question. The Commission made a great series of recommendations. We were successful in almost every one of them of substance, certainly the major ones, in convincing and wrestling part of the bureaucracy to accept what you were recommending, but also our colleagues, except when it came to congressional oversight. And this was very disappointing. And then Senator Collins and I, who are very stubborn people, I will say, normally do not yield, but the reaction had been so overwhelming that we pulled back a bit. I think that Mary Fetchet and Carie Lemack are ready to take up this battle again, and I think it is worth trying to do it because the truth is the oversight in Congress is much too diffuse and overlapping, and the consequence of that is that we are taking much too much time of the executives, particularly in the Department of Homeland Security. So I wanted to ask you if you have any thoughts about how to go at this again and about whether there is a way in which we can prioritize this. We tried

to do a lot at the outset, and we got totally defeated. But just give me your thoughts about whether you think it still is a problem—I assume you do—and whether you have any tactical suggestions about how we might take this up again, knowing that these two irresistible forces are about to focus on this.

Mr. KEAN. Mr. Hamilton mentioned why congressional oversight is so important and why it has to be effective because you are the only oversight there is, really, because the rest of us cannot know the information that you know when you are doing your oversight. And only you can say how effective it is. If Administration officials are really forthcoming in the way that they have to be when they talk to you, and if you really feel that you get every answer you want and that the oversight is effective, that is great. But we thought that it would be much more effective in a number of ways.

Interestingly enough, we have asked every Director of Homeland Security we have met: What can we do for you, how can we help you? Their first response is, Can you do something about congressional oversight?

Chairman LIEBERMAN. That is important

Mr. KEAN. Because I think it is between 80 and 90 committees now that they have some responsibility for, and they all say they are spending as much time testifying in some cases when they should be protecting us all. And preparing congressional testimony takes time, and it takes time testifying, and they are doing a lot of it. So that is extraordinarily important, and giving the Intelligence Committee some fiscal responsibility, so if the Administration is not paying attention, it will pay attention, is also, we think, very important. So we think it was a top priority when we recommended it. We think it is still a top priority, and anything that increases your ability to oversee these intelligence agencies and make them perform is a step toward protecting the country and we think a very important step.

Chairman LIEBERMAN. Mr. Hamilton, do you have any thoughts about this?

Mr. HAMILTON. Well, let me make two points. One, going back to your earlier question, how do you deal with Islamist extremism, your comments are well taken. "Know your enemy" is the first rule of fighting anybody, and I sometimes think we have a good bit of confusion on who the enemy is.

On the positive side, I want to say that in the war of ideas, I think we have made some progress, and the progress is that al-Qaeda is having a hard time. They are identified as being a violent organization that kills a lot of their own people, and I think we are making some progress there.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. And it is important progress because they have not rallied the masses to their support. So that needs to be said, but your basic point is very much on target.

The second point on the Congress—I think things happen in the Congress when the leadership does it, and they do not happen when the leadership does not. My perspective is a little more from the House, obviously, than from the Senate. And I wonder whether or not the key national security officials—the DHS Secretary, the intelligence officials, and so forth—have been able to sit down in

a congenial environment to discuss this problem with the leadership of both the minority and the majority parties. It is such an obvious thing that you weaken a department like the DHS when you have all the time that they have to spend—you have referred to—testifying. And so I think we need to focus our attention on the leadership of the bodies. They have to understand that this is a national security problem. They are not dealing here with a political problem and domestic consequences. They are dealing with trying to improve the national security of the United States, putting it on a firmer basis. I was told at one time that every single Senator sits on some committee dealing with homeland security oversight.

Chairman LIEBERMAN. You are probably right.

Mr. HAMILTON. I do not know if that is exactly right or not, but it is pretty close to it, and if it is, it is an absolute absurdity. But that is not the problem. The problem is you are undermining the effectiveness of homeland security. So, Senator, I just do not know any way to get at it except impressing upon the leadership the necessity of doing this for the national security interests of the United States. And the leadership has enormous problems in both bodies, but if I may be so blunt, they tend to look at so many of these problems as an internal political problem they have to solve in order to maintain their position in the caucus leadership. I am not naive about that. But this is a different quality problem, I believe, and we have to get that across to both party leaderships.

Chairman LIEBERMAN. That is very helpful and something for us to work on because the truth is the leaders have not made an attempt at this with everything else going on since the legislation was first considered in 2004, and the truth is they did not make much of an attempt at it then, really hardly any attempt, because they were working so hard at getting the rest of the legislation passed, that this was why take on this fight. And it is also true that the people who have the most interest in seeing this fixed, which is the leadership of the Homeland Security Department, in some sense the DNI, always have other priorities.

Mr. HAMILTON. Sure.

Chairman LIEBERMAN. It may be the immediate budget priority. It may be a legislative priority. But we have to work together to make another try at this, and I agree, it has to come from the leadership. I thank you for that.

When you were talking both about the reaction of the Muslim community but also about al-Qaeda and the ideology, it struck me that we should at least note that in the last few months there has been this remarkable development in the Arab world, in the Islamic world that is directly relevant to what we are talking about. I know that people say, well, where are the moderate voices within the Muslim world? Well, the truth is that, though we have not, I think, seen it that way, what happened in Tunisia and Egypt is really a very loud outcry by—they are not just moderate. They are not focused on religion. There may be some who are focused on religion in the movements, but the leaders in both cases—I had the opportunity with Senator McCain to visit about a month ago both countries—are very focused on political freedom, economic opportunity, and essentially getting their countries into the modern world. And they view Islamist extremism as regressive.

Now, some of them are religious, of course, but that is quite different, as we were saying before, and in some sense—I know this is hopeful thinking, optimistic thinking—what is happening now I think is a profound repudiation of the ideology of Islamist extremism, much more widespread than any of us are capable of. So that is a final statement by me.

I do not know if either of you want to comment on that.

Mr. HAMILTON. You articulated it much better than I did, but I think that is a hugely important development.

Mr. KEAN. Yes.

Chairman LIEBERMAN. And I think it really cries out to us to do whatever we can to be supportive.

Mr. HAMILTON. That is right.

Chairman LIEBERMAN. These are very proud movements. Ultimately, the people in Tunisia and Egypt, and hopefully in Libya soon, will determine their own destiny. But they may need some technical assistance and economic support. They are looking for investment from the United States. I think finally you will both get a kick out of hearing that when Senator McCain and I were in Tunisia, we met with a group of the leaders of the uprising there, and one of them said to us, "Senators, we want to ask you if you could help us to get one American who we would most like to come and speak to us here in Tunisia." And I thought to myself, "Now, who is this going to be?" And the answer: Mark Zuckerberg. [Laughter.]

Mr. KEAN. Really? Modernity.

Chairman LIEBERMAN. Well, first off, he represented the new world of telecommunications, but in some sense, Facebook had provided them with what I might call the weapons in their peaceful revolution. It is quite remarkable.

Mr. KEAN. Well, that is a wonderful story.

Chairman LIEBERMAN. Yes, I am very hopeful.

I cannot thank the two of you enough for everything you have done and your testimony. It has been very specifically helpful to focus our review that will go on for the rest of this year. We are going to keep the record of the hearing open for 15 days for additional questions and statements.

Thank you again very much. The hearing is adjourned.

[Whereupon, at 12 p.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11: IS INTELLIGENCE REFORM WORKING? PART I

THURSDAY, MAY 12, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 2:36 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Collins, and Brown.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good afternoon and thanks to all of you, particularly our three witnesses, for being here.

This is one in a series of hearings our Committee is doing this year as we approach the 10th anniversary of the attacks against America on September 11, 2001, and the purpose of these hearings is to examine how well the national security reforms implemented in the wake of 9/11 are working.

This particular hearing, of course, is being held in the aftermath of a spectacularly successful collaboration between our intelligence and military agencies that resulted in locating and killing Osama bin Laden, the al-Qaeda leader who presided, of course, over the 9/11 attacks on America.

This success required intense and focused cooperation among key intelligence agencies and the Defense Department, as well as other related agencies throughout our government.

Each organization, as we go back and are debriefed on this mission, brought its distinct assets and expertise to bear on the mission, which was to locate Osama bin Laden and then to capture or kill him. And when it comes to intelligence, sufficient material was brought together to reach informed conclusions with a level of confidence that enabled the President of the United States to make a tough call, but one that he felt the evidence enabled him to make decisively, that resulted in this remarkable success.

I do not believe that all of this would have happened 10 years ago. In fact, in the 9/11 Commission report, the authors expressed frustration that, as they reviewed our government at that time, no one was actually in charge of the hunt for Osama bin Laden, which symbolized to the Commission the dysfunction and disunity that they concluded contributed to the 9/11 attacks in the first place.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00047 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

In response to the 9/11 Commission's criticisms, this Committee drafted and Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004. There was then, and there is still today, another body of Congress called the House of Representatives, and there was another committee there that drafted similar legislation, headed at the time by one of our three witnesses, Congresswoman Harman. It results in the most sweeping intelligence reform since the creation of the Central Intelligence Agency after the Second World War.

I think the most important reform in the 2004 Act was the creation of the Office of the Director of National Intelligence, with the aim of bringing together and coordinating the efforts of our 16 intelligence agencies and offices under one leader to make sure they work toward the single goal of collecting and analyzing intelligence to better protect our national security. So the purpose of the hearing today really is to take a look at how the ODNI is doing.

I am going to include the rest of my statement in the record except to say that I feel particularly grateful that we have the witnesses that we have before us today, really three people who are particularly well prepared to assist us in answering the questions we are posing, which is how has the ODNI done and what improvements, if any, by statute or regulation are necessary.

First, as I mentioned, former Representative Jane Harman was the Ranking Member of the House Permanent Select Committee on Intelligence, where she worked closely with us, as I said, on the 2004 Act. She later chaired the House Homeland Security Committee's Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, and has now gone on to be the head of the Wilson Center, at which she is already doing a great job.

General Michael Hayden, former Director of the Central Intelligence Agency, former Director of the National Security Agency, and former Principal Deputy Director of National Intelligence, really a great, if I may say so, national asset, always a help to this Committee in its deliberations.

And John Gannon, former Assistant Director of Central Intelligence for Analysis and Production and really one of our Nation's top experts on intelligence analysis.

We thank all of you for coming today. We look forward to your testimony about where we are and where we need to go to ensure that our intelligence community consistently performs at the high levels, the kind of levels that we saw demonstrated in the hunt for and taking down of Osama bin Laden.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

I am going to follow the Chairman's lead and also do only an abbreviated version of my opening statement. Let me begin by echoing his comments about the distinguished panel that we have before us today. I, too, am particularly delighted to see former Representative Jane Harman here with us. As the Chairman has indicated, she was one of the four authors of the 2004 Intelligence Reform and Terrorism Prevention Act and worked very closely with us through extraordinarily intensive negotiations that spanned sev-

eral months. General Hayden has given so much work and effort to his country, and he also was a key behind-the-scenes player as we drafted that bill. And, of course, as the Chairman has indicated, Mr. Gannon has had a stellar career in the intelligence community. I am confident that all three of our witnesses will help us do the evaluation that we are undertaking today.

Last week's welcome news that Osama bin Laden was killed demonstrates exactly the kind of successful collaboration of intelligence and operations that we envisioned in reforming our capabilities and restructuring the intelligence community in the wake of the attacks on our country in 2001. This certainly was a great victory for our intelligence efforts and a great blow to al-Qaeda.

But the fact remains that al-Qaeda is not going away, and that is why it is time for Congress to closely examine and build upon the successes that have emanated from the Intelligence Reform and Terrorism Prevention Act, identify any shortcomings, and work to correct them and to build in further reforms.

As the Chairman has indicated, our 2004 law created the Director of National Intelligence and the National Counterterrorism Center to foster information sharing and collaboration among our security partners not only across the Federal Government but also at all levels of government.

The DNI has made some concrete progress integrating the 16 agencies in the intelligence community. I want to give just two examples of how that integration is taking place. They are not the kinds of examples that the public is generally aware of, but when you talk to those working in the intelligence community, these frequently come up.

In 2008, the DNI rolled out the innovative "A–Space," which is an intelligence analyst's Facebook. But instead of being used for social networking, our intelligence experts are posting, sharing, and asking each other about topical issues. They can collaborate with colleagues across agencies and around the world, allowing them to share leads and resources more easily than ever.

A second example is the National Counterterrorism Center's creation of "pursuit teams" that map terrorist networks, track threats using information from across intelligence agencies to bridge the gaps between national and domestic intelligence and help to put the pieces of the intelligence puzzle together.

These are just two examples of innovative ways that the stovepipes have been broken. I completely agree with the Chairman that I doubt that the kind of integrated operation that was successful in going after Osama bin Laden could have existed a decade ago. So I think that we have indeed made progress, and there are other examples as well. The arrests of Mr. Zazi and Mr. Headly are two other cases where the dots were connected.

On the other hand, this Committee's investigation and report on the Fort Hood shootings showed that we still have a ways to go in other areas, particularly in information sharing between the Federal Bureau of Investigations and other members of the intelligence community. We concluded that the Department of Defense and the FBI collectively had sufficient information to have detected Major Hasan's radicalization to violent Islamist extremism, but that the Department of Defense and the FBI failed to act effectively to-

gether on the many red flags signaling that he had become a potential threat.

So the bottom line is that almost 10 years since the attacks of September 11, 2001, and 7 years since our landmark legislation, our Nation is much safer, but we clearly are not yet safe. And that is why it is incumbent upon all of us to re-evaluate the law and to look at where we are and where we need to go.

Finally, let me just end with one comment that continues to be of concern to me. When we drafted the Intelligence Reform Act, we described the DNI as the quarterback that the 9/11 Commission envisioned and that we intended. At our earlier oversight hearing, the two leaders of that Commission, Governor Kean and Representative Hamilton, made the point that some of the functions that we envisioned the DNI carrying out are, in fact, being done by John Brennan out at the White House. And that troubles me not due to any doubts about Mr. Brennan's capabilities, but because that structure undermines the statutory role of the DNI.

So a basic question that we must ask is whether changes to the law are required or whether it is simply a matter of more fidelity to the spirit and the letter of the 2004 law in order to realize the potential of the DNI. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. Well said.

Congresswoman Harman, it is great to have you here on the other side of the table. Welcome back.

TESTIMONY OF HON. JANE HARMAN,[1] FORMER REPRESENTATIVE FROM CALIFORNIA AND CHAIR OF THE SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

Ms. HARMAN. Thank you, Mr. Chairman. I am not used to being on the other side of the table. You and I, Senator Collins, and Representative Pete Hoekstra were at the same table day and night as we crafted what is now called IRTPA, which I think is probably the worst acronym ever invented.

Again, it is a pleasure to testify with a good friend before dear friends and dedicated former colleagues who serve on one of the most important and bipartisan committees in the Senate. I now work in a bipartisan institution and pinch myself every day to be so lucky and to succeed our former colleague, Lee Hamilton, at that job. I am passionate about the topic of your hearing; intelligence and intelligence reform were the focus of my 17 years—which is 119 dog years—in the House of Representatives. I did not run an intelligence agency like Mike Hayden, and I was not a top analyst like John Gannon. But I did try to conduct, as you do, careful oversight over the intelligence function during my 8 years on the House Intelligence Committee and my 8 years on the House Homeland Security Committee.

I agree with both of you that although 24, or perhaps more, heroic Navy SEALS deserve our Nation's gratitude for the capture and kill of the world's most wanted man last week, the information on which their mission was based derived, in most part, from the

[1] The prepared statement of Ms. Harman appears in the Appendix on page 400.

integration of people and "ints" achieved by the Intelligence Reform and Terrorism Prevention Act of 2004.

We now have proof—I think we had some proof before, but we now have big-time proof that IRTPA works—that, at its best, our intelligence community can achieve the seamlessness that its authors, including me, dreamed of.

In fact, my view is that had we not passed IRTPA and had we continued to operate the intelligence community using the 1947 business model set out in the National Security Act, we would probably not have been able to thwart a number of plots or take down Osama bin Laden.

Let me focus briefly on three issues: First, both of you have addressed the performance of the Director of National Intelligence. By the way, I take credit for the name of DNI. Originally, it was supposed to be National Intelligence Director, which I thought sounded like a bug.

Chairman LIEBERMAN. It is interesting. I take credit for that, too. [Laughter.]

We probably had the same thought.

Senator COLLINS. And I am the one who actually did it. [Laughter.]

Ms. HARMAN. It was a good start.

Chairman LIEBERMAN. I think we can all agree that Pete Hoekstra had nothing to do with it. [Laughter.]

Ms. HARMAN. Moving along, second, let me talk about something Senator Collins mentioned, which is the role of domestic intelligence agencies and, third, some ongoing issues involving congressional oversight—of course, not involving the two of you.

As for the DNI, I think the DNI continues to be a work in progress. Congress intended her or him to be a joint commander. A quarterback is a good analogy, but I recall our modeling this after the Goldwater-Nichols law that created the joint command across four military services, and it works very well, I believe, at DOD. So we envisioned a joint commander, not a huge bureaucracy by a joint commander across 16 intelligence agencies—far more than a coordinator, and a job that clearly required leadership skills.

IRTPA is not perfect, but I believe it contains adequate authorities to give the DNI the necessary leverage she or he needs to get the job done. I have often said that the function is 50 percent law and 50 percent leadership.

Congress intended, as I think both of you said, that the DNI serves as the principal intelligence adviser to the President. Those authorities were, I think, clarified and enhanced when the President, President Bush, issued Executive Order 12333, and that was the intention of Congress and clearly the intention of President Bush as well. This has never really happened. I believe that during the Bush Administration, Vice President Cheney was the principal intelligence adviser, and as Senator Collins said, during this Administration, John Brennan, the counterterrorism coordinator in the White House, is the principal intelligence adviser. In my view, neither President has adequately valued the DNI role, nor has either President made an adequate effort to support the mission. This is something I think Congress and those of us who agree with

Congress should push harder on. It is not to diminish the reputation and power of the people in the White House who have assumed the role, but we established a person who is confirmed by Congress and accountable to Congress to take that job, and I think we should push harder to make certain that person actually has the full job.

Let me raise a few issues that I think are important that the DNI is addressing.

First, DNI James Clapper has suggested—and I would urge that this happen—that the National Intelligence Program be taken out of the Defense Department and added to the DNI's budget. I think that this will achieve more efficiency and promote more accountability.

Second, I think the issue of right-sizing the DNI staff is being handled well, and we should move on to other topics. We should also, by the way, reduce the use of outside contractors.

Third, when General David Petraeus moves to the CIA role, and CIA Director Leon Panetta becomes the Secretary of Defense, hopefully we will finally cement a good working relationship between the CIA Director and the Secretary of Defense. This was impossible in 2004 because the Secretary of Defense Donald Rumsfeld implacably opposed the law and the then-Chairman of the House Armed Services Committee, Duncan Hunter, also did. We had to work around them to achieve what we did, and I thought it was pretty darn good.

And, finally DNI Clapper urges that we reduce the number of reports to Congress. I know how those reports get into statutes, and I know what they mean politically to the members who add them. But I think consolidating them will save time and resources and enhance the focus on the mission.

I want to keep to my time, so let me just move to another subject, and that is, our domestic intelligence agencies. I think, as Senator Collins said, that there are ongoing problems with vertical intelligence sharing. This is going better, especially because you are doing some great oversight. I think that the Fort Hood massacre, as you said, could have perhaps been prevented if there had been better collaboration between DOD and the FBI, and the especially weak player is the intelligence and analysis function in the Department of Homeland Security. We need much more work, and I want to thank your staff and you for the work you did on helping to pass the reducing overclassification bill last year, which was signed into law by President Barack Obama in October.

Finally, on congressional oversight, this Committee, your Committee, has far more jurisdiction than its House counterpart on which I served for 8 years. But I do not believe either committee in the Senate or House has adequate jurisdiction. We know why this happens. No one wants to give up any jurisdiction. But I actually think that reorganizing this function in the Congress would, one, carry out a strong recommendation of the 9/11 Commission; but also, two, give us a much better shot of providing the oversight necessary to be sure that the intelligence community will get the job done and help us protect our homeland.

I agree with Senator Collins that while last week's news is fabulous, it will not diminish the threats to our homeland, and it prob-

ably will not diminish the potency of al-Qaeda, although that potency I believe will now move from Pakistan to other places like Yemen, where al-Qaeda in the Arabian Peninsula, is emerging, in my view as the part of al-Qaeda that is doing the most work both to inspire and train people to attack us in the homeland.

Let me finally conclude by saying that there is no way to make our homeland 100 percent safe. What we can do is minimize risk, and we are doing that. We need to constantly re-evaluate the threats against the United States and to prioritize our investments. We are not making a lot more brain cells. Those that we have have to be applied against the top threats, and surely we are in a resource crunch, and our resources must be carefully marshaled.

Let me close by recognizing the heroically brave women and men of our intelligence community who put their lives on the line every day for our country—often in austere places around the world, living apart from their families. Surely CIA Director Panetta, DNI Clapper, President Obama, some Members of Congress, and others, should take a lot of credit for last week's activities. But the true heroes were those in the field, not just the Navy SEALs but those in the field who put together the clues that led to the information, that tracked the couriers, that found the house, that found Osama bin Laden, and they deserve our heartfelt thanks. Thank you.

Chairman LIEBERMAN. Hear, hear. Thank you. And if I may, that gave the President a sufficient level of confidence in the information he had to order that the raid occur. Thank you for that excellent statement.

General Hayden, it is great to welcome you back. Thank you for being here, and we look forward to your testimony now.

TESTIMONY OF HON. MICHAEL V. HAYDEN,[1] FORMER DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY AND FORMER DIRECTOR OF THE NATIONAL SECURITY AGENCY

General HAYDEN. Thank you very much, Mr. Chairman. Good to see all of you again.

Let me begin by attempting to scope the problem. We sometimes look as if we are trying to repair a community that was totally dysfunctional, and what I want to describe is I think what the legislation attempted to do was to balance two things, both of which are virtues, and two things which any complex organization has to balance, and that is, simply the unity of effort for the whole and autonomy of action for the parts. And both of those are good things. Both need to be protected. And I think the macro judgment was that we were more than a brick shy of a load when it came to unity of effort for the whole, and that was the intent of the legislation.

The real problem is, I think, what we are trying to do is to build what some of our younger analysts and case officers would describe as a networked organization, which very frequently looks and acts like it is leaderless or has many leaders. And, unfortunately, the only way we can get from here to there is to actually have very strong leadership in order to create this kind of organization.

[1] The prepared statement of General Hayden appears in the Appendix on page 403.

And so what the Nation decided and what you sponsored and fostered in 2004 was another path to that balance, not the DCI path but the DNI path.

I think those of us in the community were a bit nervous about that. We were quite busy at the time. We actually thought that the DCI had some real authorities and did provide a fair amount of glue. But even those of us who had our doubts recognized that if we needed more glue, if we needed more unity of effort, the then current model, the DCI, was probably going to be inadequate simply because the DCI had full-time day work as the Director of the CIA, and it would be very hard for anyone, almost superhuman, to reach above that role and both psychologically and physically play the role of coaching the entire community.

But you had a real daunting challenge on your hands because whatever glue we had in 2004, whatever centripetal forces we were able to create in the community, came from the fact that the head of the community, the DCI, also headed the CIA, and that "C" still meant "central" and that he was in that core position inside the community. And, of course, the decision was made, whatever else the DNI was going to be, he was not even going to have his office at Langley let alone run the CIA. So you really had a difficult challenge to pull us out of this course, put us on another, and put enough bricks in his backpack that he had enough authority to get beyond what the old model had provided us.

Beyond that, as existentially difficult as that was, this has actually been harder than it should have been. We were at war, and, therefore, it is kind of hard to restructure when your daily operations tempo is so important. But there is another, I think more subtle challenge because we are at war. Three or four of those really big organizations that you care a lot about, and most of whose first initials are "N," are actually in the Department of Defense. As mentioned, I was the Director of NSA, and I would not say we were schizophrenic, but we did have a duality in our personality. We were the National Security Agency, but we were also directed to act as a combat support agency.

In many ways, your law was trying to strengthen the national character, to bring folks, organizations under the Director of National Intelligence. It is inevitable that after 9 years of war, the combat support character of those organizations becomes more and more dominant. There is nothing wrong with that. That is actually a good thing. We would all agree, we would all foster it. But it is not quite a convergence with the course of action that you set out in terms of strengthening the DNI.

There are other things that made this harder. We have had four DNIs in 6 years. That cannot help. We have had four DCIAs in 6 years. That cannot help either. I think one of the most powerful phrases in your legislation was the role you gave to the DNI to recommend the DCIA to the President. I just told you we have had four and four. I can think of only one example where the DNI actually recommended the head of the CIA to the President of the United States, and that was John Negroponte recommending me to be DCIA instead of his Deputy, and we overlapped for only 6 months after I took that job. That is actually pretty important.

And, finally—and I am fearful of being too self-referential here—my old job, the PD–DNI, the Principal Deputy, I think is really important because those two tasks you gave the DNI, senior intelligence adviser to the President and smooth functioning of the intelligence community, those are really hard. And that deputy function is really important. For over half the life of this legislation, that deputy position has been vacant. That has real impact on, I think as you said, Senator Collins, effecting the intent of the law rather than trying to change the legislation.

Now, all that said, I think there has been some really good news with regard to the DNI. It exists and is accepted, and, frankly, in 2005, when I was Principal Deputy, that was not a given throughout the community.

The NCTC has already been mentioned as a signal success, and I think that is right, and there will probably be questions on it as we go further.

Imagine, if you will, trying to create the NCTC, which fundamentally is characterized by the mingling of foreign intelligence with domestic law enforcement. Try to picture that if it reported not to the DNI, but if it reported to the DCI, who was also the head of CIA, and therefore, was your foreign espionage chief. American political culture would have rejected that like a foreign object. And so the DNI structure has actually enabled the success of the NCTC.

The DNI has also kind of thrown his body from time to time in front of really big trains. I can recall Director Mike McConnell spending about 18 months on legislation with which you are all familiar—FISA reform. That could not have been done by any sitting Director of NSA. Only the DNI could have brought the gravitas of the community to that discussion.

This again sounds a bit personal, but it is very real. Every day I was a DCIA, I thanked God there was a DNI. I had no idea how anybody could be a DCIA and also be head of the American intelligence community. You talked about the recent success and used the term "quarterback." I think I am a little more comfortable with the term "coach" to describe the DNI. And I think it is clear—I was not on the inside, but from all the accounting, I think it is clear that Director Panetta was the quarterback for this effort.

There is an echo of that—if you recall al-Kibar, the Syrian nuclear reactor in eastern Syria that was ultimately destroyed. When that came up, Director McConnell and I worked very closely, but he, in fact, empowered me to act on behalf of him because this was at the operational level. And I do not know that we want the DNI routinely playing at that level.

There are other things the DNI has set in motion. Sharing in something that is called ICD File 502, which sounds like coded language to most folks in the room, but it is a process which allows over time the bureaucracies to more readily, more facilely share information. Joint duty is another thing that has been set in motion and that over time will change the culture of the community. Not possible without the current structure.

There probably are some tinkerings in the law that someone might consider. I will not suggest any. I think that should come out of the sitting DNI. But some things that come to mind, if there is anything you need to do to get the National Intelligence Program

more fully under the DNI and out of the DOD budget, if there is some legal impediment I am not aware of, that is probably a very good thing.

We have already mentioned that we are cooperating pretty well east to west at the national level. But the new threat is going to require more cooperation north to south. And how better do we share between national, State, local, and tribal assets? I do not know that there are legal impediments, but if there are, I think that would be a great help.

All that said, I think I agree with something that both of you suggested. We are going to succeed or fail more on intangibles than we are on the precise letter of the law, as important as that is. The three intangibles that most come to mind to me are:

First, the personality of the DNI. That really matters, who that person is.

Second is the relationship of the DNI with the DCIA. That has got to work. My shorthand is the DNI owes the DCIA room to run, and the DCIA owes the DNI total transparency.

Then finally, as already suggested, whatever shortcomings there may be in the law, everything is fixed if the DNI is—and everyone knows him to be—the President's senior intelligence adviser without question.

Thank you very much, and I look forward to your questions.

Chairman LIEBERMAN. Thanks very much, General Hayden. That was great.

Mr. Gannon, thanks again for being here and please proceed.

TESTIMONY OF JOHN C. GANNON,[1] FORMER DEPUTY DIRECTOR FOR INTELLIGENCE AT THE CENTRAL INTELLIGENCE AGENCY

Mr. GANNON. Thank you very much, Mr. Chairman. I will also summarize the statement I provided for the record.

In my view overall, the performance of the U.S. Intelligence Community has improved dramatically since 9/11. Analytic and operational tradecraft have advanced significantly. Performance in counterterrorism programs has reached the highest standard of professionalism and dedication. The application of technology has broadened, deepened, and accelerated. Interagency collaboration, especially in support of the warfighter, has improved markedly. And progress toward a more distributed model of intelligence support to users anywhere in the world is palpable and encouraging. The fusion of intelligence, the synergy of well-trained people and advanced technology, and the interagency teamwork in Afghanistan and Iraq are at their highest level ever—a level that seemed unattainable when I left government.

The creation of the DNI has contributed significantly to this progress, but other leaders and individual agencies—with administration and congressional support—also have taken impressive steps on their own. The Department of Defense won congressional approval to establish in 2002, the position of Under Secretary of Defense for Intelligence to improve management of its considerable intelligence assets and programs. Most significantly, in my view,

[1] The prepared statement of Mr. Gannon appears in the Appendix on page 406.

the Secretary of Defense elevated the authority and boosted the budget of the Joint Special Operations Command to provide in the field a strong coalescing leadership, a clear chain of command, and a powerful authority to coordinate focused requirements for intelligence collection and analysis. I would risk the outside judgment that the cooperation of CIA, including its Counterterrorism Center, with the JSOC has never been closer or more effective. While there is always room for improvement in the intelligence business, the strong, collaborative performance of our agencies "down range" today is unprecedented and a source of justifiable pride for the intelligence community.

The domestic picture, in my view, is mixed. The key difference with "down range" is that there is no JSOC counterpart in the homeland to integrate intelligence processes and products. The FBI has built an impressive intelligence infrastructure and has shifted significant resources, once wholly devoted to law enforcement, to domestic intelligence collection and analysis. The National Counterterrorism Center has made significant progress in integrating foreign and domestic intelligence and analysis. The Department of Homeland Security, with its 22 constituent agencies sometimes taking initiative on their own, has made commendable strides in border security and some, but uneven, progress in sharing threat-based information and coordinating policy with State and local governments and the private sector. Overall, however, domestic agencies do not show the strong unity of effort that is evident in theaters of conflict abroad. Domestic intelligence and security is a much slower work in progress.

The DNI should be seen as a leader with explicit responsibilities for clearly defined oversight of IC performance, for the development and application of interagency program standards, and for the implementation of the National Intelligence Program. We are not yet there, in my view. I believe, however, we can do much better. We should recall that the IRTPA was passed into law after decades of debate about the inability of successive DCIs to manage the intelligence community. The IC today is challenged by historic geopolitical change, a globally dispersed threat environment, and a technological revolution that is enabling even minor adversaries to hurt us as never before. The DNI has the potential to help agencies to achieve a unity of effort in this challenging environment.

To be optimized, the DNI roles and responsibilities should be tied clearly to defensible IC strategic priorities and requirements. The DNI's leadership must be authoritative with regard to these IC-wide priorities but not intrusive in agency-specific matters. It must recognize the distributed and networked nature of intelligence support around the world today. And, most importantly, in my view, the incumbent must have the visible and sustained backing of both the White House and the Congress, and it is questionable whether the DNI has this now. This in my judgment has been a major obstacle to progress.

The DNI may need additional authorities. I believe his management of the NIP, for example, would be strengthened if it were moved from the defense budget to the ODNI. In a period of tightening budgets, he will need clearer authorities and powerful top

cover to evaluate and prioritize key programs for growth, reduction, and elimination, a role he has a unique potential to perform.

At this juncture, however, rather than simply add authorities, I believe it would be more useful in a period of IC leadership transition to take a step back and consider ways to get the intelligence community, White House, and congressional priorities aligned to enable and support the DNI on this hazardous mission.

I would cite several priority areas in addition to the NIP management and cross-agency program evaluation on which the DNI is uniquely positioned to help improve IC performance and enhance U.S. national security:

Balancing strategic versus tactical collection and analysis, which in my view has gone too far in the tactical direction.

Equipping trained analysts for the Information Age, meaning giving them greater and full Internet access to social media and to outside experts, which I think is essential against the challenges we face today.

Strengthening commitment to science and technology in an era when we are subject more than ever to technological surprise.

Enhancing training and education for the intelligence profession—that is, with a curriculum that codifies and conveys the body of knowledge that defines the intelligence profession itself.

Adapting security and counterintelligence to the 21st Century, pursing the benefit from innovation and avoiding the costs of doing it the old way.

And continued promotion of information sharing across all the agencies, and improving intelligence community procurement strategies and policies as well as improving government contract management overall.

I am glad to say that the DNI is working on all these important priorities, but in my judgment, he will need help to deliver the best results. And it should matter to all of us that he succeeds.

Thank you.

Chairman LIEBERMAN. Thank you, Mr. Gannon. Your statement and the others prepared will be part of the record, and we appreciate the time and thought that you gave to your statements.

We will do a 7-minute round of questions here.

General Hayden, I think I want to start with you, picking up on one thing you said, reminding us that the DNI has two major functions: One is to be the senior intelligence adviser to the President, and the other is to be, whatever term we choose, coach, manager, leader, quarterback, of the intelligence community.

You have been pretty close to the functioning of the DNI since it came into effect, and first I want to say that you are absolutely right. One of the shortcomings over the last period of time, which is not in the law but in its implementation, is that for too long the Principal Deputy position at the DNI has been vacant, and that really means that either we are putting these two functions in a very burdensome way on the DNI himself, or he is not going to be able to do the two. And either he is going to do both not as well as it should be done, or he is going to fail in one or not do as well as he should.

How would you assess the function of the DNI as the senior intelligence adviser to the President in practice? You talked about

this a little before. The CIA is a big agency with a lot of history and a lot of assets, so that is the muscle they have. But from what you know, to the extent you can talk about it from the inside, has the DNI actually ended up being, since we created the position, the senior intelligence adviser to the President?

General HAYDEN. I think it has gone back and forth. It is very much dependent upon the personality of the President and the personality of the DNI.

The first thing is the DNI has to choose where he is going to shift his weight. Does he shift it downtown? I mean, that is, frankly, how to draw the picture. Or does he shift it back out at headquarters?

There is an incredibly powerful gravitational pull downtown, and that is not out of pride from the DNI. That is out of the demand of the President and the National Security Council staff.

My experience, to show you how difficult this was, I was generally always there—not in the morning briefings. That was generally a DNI show. But a lot of decisions get made at the Deputy's level, the Principal's level at the NSC, and I was almost always invited. And so I am there with Admiral McConnell. Literally, the President or Steve Hadley would say, "OK, the two Mikes, you go first." And Mike McConnell would talk, and then if I had anything to add, I would add. But we were both there.

Admiral McConnell was really disadvantaged. I am sitting on top the Nation's premier analytical service. Admiral McConnell is up the road reading books. I am putting somebody in the back of the car with me explaining the details we are running down because I have the analytical staff to do that.

Chairman LIEBERMAN. Sure.

General HAYDEN. So there is a bit of a tension there, a bit of an anomaly. But you have to work through it. Remember that transparency and freedom of action between the two? The DCIA and the DNI have to be friends, and the DNI does not get to do job two, which is smooth functioning of the community, unless everyone believes he is the one responsible for job one. He gains power for the second task from his performance of the first.

Chairman LIEBERMAN. I agree. Obviously we wanted the DNI to be the principal intelligence adviser to the President because the gathering of intelligence goes beyond the Central Intelligence Agency, even though it has the most personnel and the most assets in the community.

Is the DNI's presence at the daily intelligence brief to the President critically important to this fact? I mean, that is not in the statute. Well, it is, actually, generally in the statute. But there is latitude.

General HAYDEN. First of all, Mr. Chairman, this depends on the personality of the President. All presidents deal with this in a different way. President Bush was very interactive, was face to face, it was that human contact. I think President Obama is a bit more cerebral and likes printed material and so on.

Chairman LIEBERMAN. Right.

General HAYDEN. So you have to accommodate the character of the President. But I do think it is very important—let me be very precise—that the DNI be represented in those morning briefings,

either he or the Deputy. But on balance, I think it needs to be the DNI more often than not.

Chairman LIEBERMAN. Congresswoman Harman or Mr. Gannon, do you want to get into that discussion about the interplay of the senior adviser to the President and coordinator of the intel community? Ms. Harman.

Ms. HARMAN. We have seen good stories and bad stories. There was a tension between DNI Dennis Blair and CIA Director Leon Panetta that wasted a lot of time about what you call people who are forward deployed in our embassies. I thought that was a stupid fight, I really did, and certainly nothing we imagined when we formed the law.

It seems to me that, as I said in my testimony, the DNI role has never been adequately valued by either president during the time of the law, either President Bush or President Obama, and that is something we should push for.

But, second, my term at the DNI is the joint commander. I think her or his job is to leverage the strengths of the other agencies. If you are a good CEO, you do not do all the work yourself. You help those underneath you understand the mission and perform their missions well, and then you pull it together, and that is what I see is the DNI role.

Yes, I agree with General Hayden that being part of the President's daily brief is important, but I do not think the DNI personally has to do it every time. Again, letting other people shine and have that face time, too, is the sign of a secure leader.

Chairman LIEBERMAN. Right. You have said twice now that we ought to be pushing harder in the face of the fact that neither President who has had a DNI yet has used that DNI to the full extent that we hoped. Are you thinking additional statutory authority to the DNI? Or is it more trying to make the point to the President, if we could, that this is what we intended and this will serve him better?

Ms. HARMAN. Yes, it is the latter. I think that to the extent that our law left any ambiguity—and, of course, as one of its authors, I thought it was quite swell—that was clarified by——

Chairman LIEBERMAN. But not without ambiguity.

Ms. HARMAN. In the face of implacable opposition by two key people in the government at the time, I thought we did extremely well. But Executive Order 12333, issued by President Bush and supported at the time by then-Candidate Obama, as I recall, was an attempt to make even clearer that we intended the DNI to be the principal actor in intelligence.

I mean, you cannot make a President rely on somebody in the chair, but as General Hayden has said, you can try to help forge the right chemistry between the President and this person. And you could also explain as Congress that the person accountable to Congress for the failures or successes is the DNI, not the Vice President of the United States or the principal counterterrorism officer in the White House.

Chairman LIEBERMAN. Mr. Gannon, do you want to get into this?

Mr. GANNON. As the former Deputy Director of Intelligence who ran the PDB staff at CIA, I always regarded this daily access to the President of the United States as critical to the intelligence

mission and absolutely essential to the role of a senior intelligence adviser to the President.

By the way, I will add—and I think Mr. Hayden knows this well—that it takes tremendous analytic resources to perform this role successfully. The substantive role that one plays in the PDB forum is very different from the management roles in the intelligence community. All DCIs struggled with this tension, and all of them ultimately failed at trying to perform the two functions.

But I think the problem with the DNI construct now is that the DNI does not have adequate analytic resources to serve him in the substantive role. What it takes to produce that book every day is a tremendous investment of resources and expertise, and they have to be serving the person who actually provides the briefing or whose deputy provides the briefing.

Chairman LIEBERMAN. So is the answer to try to provide more analytical resources to the DNI?

Mr. GANNON. That would be my answer to the question, yes. I think if the DNI is going to continue to serve in that substantive role, he needs to have more resources to do the job.

Chairman LIEBERMAN. Because, otherwise, this will naturally move to the CIA because they have the analytical——

Mr. GANNON. I think there would be a very strong gravitational pull in that direction.

Chairman LIEBERMAN. OK, thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

As I am listening to this debate, it reminds me that in Washington there are really three levers of power. One is your relationship with the President, and we have talked about the fact—and I agree with Representative Harman—that neither President Bush nor President Obama has fully valued the DNI as the principal adviser to the President the way we intended in the law. The second is control over personnel, and I want to come back to that with an example. And the third is control over budget.

Now, each of you, I believe, made a budget recommendation to us. When we wrote the 2004 law, there was a huge dispute over whether the intelligence community's budget should remain with DOD and then be doled out, essentially, to the agencies or whether it should go through the DNI. And I think—but I want to clarify—that each of you are recommending more authority for the DNI in this area. So if I could first explore the budget issue and start with Representative Harman.

Ms. HARMAN. Yes, moving the so-called NIP into the DNI's orbit is an active recommendation made by the current DNI, Jim Clapper, and I think it would be very helpful. I have not thought about whether that requires a change in the statute. I am not sure of that. I do not think we know—or what the answer is now? We do not know. Imagine that. We do not know.

But I am one, as I said, who thinks that this is 50 percent law, 50 percent leadership, so I think we can accomplish a lot of what we are trying to achieve unless there is a bar in the statute by just getting, hopefully, this President to support DNI Clapper's recommendation.

Chairman LIEBERMAN. I have been advised that we have actually been in discussion with the DNI about whether there is a need for

statutory action, and they are not sure. So they are coming back to us with an answer, and then we will reason together.

Senator COLLINS. General Hayden.

General HAYDEN. Yes, ma'am. You have some tension inside the law on the budget.

Senator COLLINS. Yes.

General HAYDEN. The verb you picked is great. "Determine" is what you decided. And then you have Section 1018, which says nothing in here infringes the prerogatives of the cabinet officers in which these organizations are located. I am not suggesting to go back in and use a wrench to change any of that, but to the degree you can in the process foster "the DNI determines," I think that is a very positive thing.

In terms of shifting the National Intelligence Program out of the DOD budget and into an independent account under the DNI, I think most people who look at that say it would actually strengthen his authorities in the execution year, which is not a bad thing. It may not do a whole lot in the planning or programming year. But in the execution year, which is where you kind of look around and say who is burning money at the rate they expected and who is not, and let me remind everybody, it was my money to begin with, that actually might be a very positive thing.

Senator COLLINS. Mr. Gannon.

Mr. GANNON. I agree with all that has been said. I think Jim Clapper has made a very persuasive case that I would have probably agreed with even before he made it. And I think in an era now of greater stress on the intelligence budget, I think it is important in real terms and also symbolically—that he have that budget control.

Senator COLLINS. I was smiling as General Hayden was talking about the language because I remember how difficult it was and that we did want the DNI to be responsible for determining the budget. But in order to get the bill through, I think we did create a compromise or some lack of clarity in order to get the bill accomplished, which sometimes happens. So it will be interesting to see if we can perhaps clarify this.

Let me turn to the personnel issue. As Representative Harman has mentioned, at the start of this current Administration, shortly after Leon Panetta was confirmed as the CIA Director, the DNI, Admiral Blair, issued a directive in which he claims the right to select an individual other than a CIA station chief to be the DNI's representative in foreign governments. And this built upon similar but far less public efforts that were undertaken by previous DNIs Negroponte and McConnell as well.

But this did blow up into a rather prominent public battle between the DNI and the CIA Director, and the unfortunate, in my view, outcome was the White House was forced to choose sides and sided with the CIA, which in many ways, in my view, undermined the DNI's ability in the whole area of personnel.

Who should be in charge of the personnel in the intelligence community in terms of allocating assets? Mr. Gannon, we will start with you.

Mr. GANNON. First of all, I think that the particular case that you are citing was badly handled. The outcome need not have been

what it was. I believe that it could have been managed in a way that all parties to this conflict could have gone away with a much better feeling. But I think it ended up publicly undermining the DNI and doing a lot of damage to his effort to establish authority.

I think that, because of the nature of the complicated and fast-moving global threat environment that our country now faces, the intelligence community needs to be able to move assets, including personnel, quickly and the DNI must have the authority to do this. I do not have the confidence to say how precisely this should be crafted into law, but I think the DNI is the appropriate leader to have this authority.

Senator COLLINS. Thank you. General Hayden.

General HAYDEN. Yes, ma'am. Admiral McConnell and I had that very issue for quite a while when we were in office and, unfortunately, just could not get it across the finish line. This is a very emotional issue for CIA, and I was doing my duty in terms of representing the Agency's views, and very frequently my senior staff would say, "You need to take this to Mr. Hadley," or someone else in the White House. And my response was, "Guys, we take this to the White House, we lose." I mean, there is no way the White House cannot support the DNI in this kind of issue.

Now, frankly, I think the DNI was wrong. I think it should be the station chief. I think our foreign partners expect it to be the station chief. But the DNI has a right to be wrong without being overruled in such a public, humiliating way by the White House. So I agree with Mr. Gannon. It was a very bad thing.

In terms of moving personnel around in general, falling back a little bit on the military model, commanders talk to commanders. All right? Commanders do not command troops inside other people's organizations. So I think the model we might want to think of is to make sure the DNI has the authority to demand capabilities of his component commands, and his component commands are NSA, NGA, CIA, but to leave those component commanders the freedom of movement to how they respond, how they create that capacity where the DNI wants it. But he fully should have the authority to demand capacity where he needs it.

Senator COLLINS. That is a good distinction. Representative Harman.

Ms. HARMAN. I strongly support that last point and also agree with Mr. Hayden's earlier point that the DNI should carefully pick her or his fights and hopefully pick the right fights. This was the wrong fight.

All of this feeds the conversation we are having, we have been having from the start. I felt, again, given the implacable opposition by Secretary of Defense Rumsfeld and House Armed Services Chairman Duncan Hunter, that we did pretty well. We consulted closely with an unnamed source then in the Bush Administration to make sure we had adequate authorities for the DNI to build the budget, not just to execute the budget because moving money, providing money, is how you give somebody power. And I believe we had adequate authority there. That Section 1018 was modified or clarified later by Executive Order 12333, so I am pretty confident that the budget authorities are OK.

In terms of people, even people for the PDB, if I were the DNI, I would use assets that exist among the 16 intelligence agencies to help me do what is necessary there. There are excellent analysts at the CIA, as has been mentioned. John Gannon knows that extremely well. And they surely were very good at providing information leading up to the capture and killing of Osama bin Laden. So those assets can be used by the DNI. There is no prohibition against using them. They do not have to move to a different box. I think we should be done with moving boxes around, and we should insist that the DNI get the respect that person deserves and do the job by leveraging the assets of the agencies under her or his command.

Senator COLLINS. Just one final comment, if you will indulge me. I also believe that if the intelligence community more fully adopts the joint model of the military where in order to advance your career you need joint service, that will help promote those kinds of exchanges and willingness to give up talented people as well.

Ms. HARMAN. Senator Collins, that was in the law.

Senator COLLINS. Oh, I know.

Ms. HARMAN. Giving some points for joint service and trying to break down, as you said, the stovepipes and promote a need-to-share culture instead of a need-to-know culture.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

One of the other ways in which the law attempted to give the DNI authority in a way that would help him or her be a better manager or leader of the intelligence community was in the recommendation of personnel throughout the intelligence community.

General Hayden, just as the beginning of a series of questions, you made, I think, a very good point, which is that, to the best of your knowledge, the only CIA Director who was actually recommended by the DNI was yourself. And in the other cases, I assume what you are saying is the name came from the President. And while the DNI may have formally put his name to the bottom of the letter recommending, that is the way it happened.

General HAYDEN. That is my understanding, Senator, and, frankly, there is nothing wrong with that in an objective sense.

Chairman LIEBERMAN. Yes.

General HAYDEN. But if you are going to establish that kind of relationship—if you have this ideal relationship between the DNI and the DCIA, starting off with the one owing nothing to the other for being in the position is not a disqualifier, but you are not getting out in front of the pack either.

Chairman LIEBERMAN. It makes it harder. You are absolutely right. Probably none of us here thinks that General Clapper came up with the idea of General Petraeus being the head of the CIA. [Laughter.]

Not that he is opposed to it. I have talked to him about it. I am sure he is happy with it.

This discussion is another piece of evidence, this one that we have just had, of the way in which the law can express an aspiration that the Congress has regarding something, but it all depends ultimately on how the people in the positions implement it.

So acknowledging that piece of unaccustomed congressional humility, let me go on to ask you, one other idea that has been suggested to us as we take this look back at the DNI is that we ought to extend the authority of the DNI to approve—recommend and/or approve personnel throughout the intelligence community below the level of the head of the constituent agency, perhaps down to the second or third position in the agency.

What do you all think about that? Let us start with Mr. Gannon.

Mr. GANNON. I would think that is an idea whose time has not yet come. [Laughter.]

Chairman LIEBERMAN. General Hayden.

General HAYDEN. No, that did not have any particular charm for me either, Senator.

Chairman LIEBERMAN. Yes. Representative Harman.

Ms. HARMAN. I think there are higher priorities, like urging the President to fully stand up the Privacy and Civil Liberties Board, which is required under the law. I would go there before I would start an opportunity to pick new fights between the DNI and other agencies.

Chairman LIEBERMAN. Am I right in interpreting the reaction of you to be that actually consistent with what we have just said about the DNI relationship to the DCIA, the head of the constituent agency ought to be able to choose his own second and third people?

Mr. GANNON. Yes.

Chairman LIEBERMAN. Just in terms of their ability to work together.

Let us go back to this extraordinary experience we have just been through with the intelligence leading to the takedown of Osama bin Laden. The President designated the Director of the CIA, Director Panetta, under Title 50 to be in charge of this operation, even though in the end—and Leon Panetta both privately and publicly has gone out of his way to say that he then essentially delegated the final part of it to a Title 10 force, which was the Special Operating Command under Admiral William McRaven.

I suppose the first question I want to ask is whether, consistent with what we have been focused on today—I know this is second-guessing on a spectacular success, but whether the President, consistent with the intention of the law we are talking about, really should have designated the DNI to be in charge of the hunt for Osama bin Laden as opposed to the DCIA. Ms. Harman, do you want to start that? We will just go down the row.

Ms. HARMAN. In organization chart terms, I think the answer to that is yes. I think this was a highly risky operation, and there were at least plausible reasons to designate someone else. I am just guessing that the President has worked longer with Director Panetta than he has with DNI Clapper on a personal basis and figured he not only brought a lot of the assets to the table in terms of preparing the information on which the special ops team acted, but he also had a strong relationship with Congress and, therefore, that made him probably the best guy, especially in the event that something went wrong. And so I think this was a call based on personal chemistry more than on an organization chart, and I do not fault the President for making it, and the result was spectacular.

Chairman LIEBERMAN. And it worked.

Ms. HARMAN. Yes.

Chairman LIEBERMAN. General Hayden.

General HAYDEN. All that is true and I agree with it, but I do not think it is exclusive. I think it is structural. It is just not personality based.

If you do it under Title 50, it is a covert action. Executive Order 12333 says—the President can change this, but what it says right now is the only organization of the U.S. Government that conducts covert action is the Central Intelligence Agency. So I understand why that has gone in that direction.

I think technically Director Panetta had what is called OPCON, which means he is ultimately responsible for it, but he gave Admiral McRaven and his troops TACON. It makes great sense. I cannot think of any other way of doing it.

With regard to the DNI role in this—we actually had this discussion in the Bush Administration, and I know Congresswoman Harman has talked about needing more presidential oomph to the job. We actually got a fair amount from President Bush based on my recollection. We had a pretty serious debate about this role, and we went to the law, and the language in the law is that the DCIA reports to the DNI for all the activities of the Central Intelligence Agency. And that is the verb: "reports." It is not "authority," "direction," or "control," which are also English words that were available, but they were not chosen.

The ultimate decision—and we had this discussion long before going to Abbottabad—is that the DNI has to have total transparency. But covert actions are so sensitive, so delicate, that the President—and I suspect this President—wants no one between him and the individual carrying out the covert action. And so in that sense the DNI is here to offer views as a member of the NSC and in an advisory role but not in that chain. We discussed this at great length. We really clearly did not want to make this two hops rather than one.

Chairman LIEBERMAN. Discussing, in other words, this kind of action.

General HAYDEN. That is correct. Title 50 covert action.

Chairman LIEBERMAN. Right. And, again, because the CIA Director is in charge of the operators here.

General HAYDEN. That is correct.

Chairman LIEBERMAN. Right. Mr. Gannon.

Mr. GANNON. I have no problem with the way this transpired, and I do not think it really had any negative impact on the DNI's authorities.

As a professional intelligence officer, I always regarded covert action as only partially an intelligence activity. It is supported by the National Intelligence Program, so the DNI should play a consultative role. But I think the accountability for covert action belongs so acutely to the President that there should not be any layers between him and the CIA Director.

Chairman LIEBERMAN. Again, if I may go over my time, I am going to ask you, Mr. Gannon, a somewhat related question. I was interested in your statement in your testimony that the intelligence community has moved to what you called a more distributed model

of providing intelligence support in which a large number of intelligence agencies and offices provide direct support to policymakers and also work closely with the military—in fact, with troops on the ground—and that there could be a conflict between that model and having a strong central leadership. And I just want to ask you to develop that a little bit more.

Is there necessarily a conflict there? Isn't there an argument that DNI should in any case be the leader ultimately responsible for building the distributed network and ensuring that it works properly and, of course, is ultimately accountable for its performance?

Mr. GANNON. The direct answer to your question is I do not think there is necessarily a conflict. My point is that I think we do need to understand the evolution of the intelligence community to a more decentralized distributed model of intelligence support over the past several years. It is not going back.

Back in the 1990s, when I was managing intelligence analysis there really was a preference for the national customer at CIA, and I could——

Chairman LIEBERMAN. Meaning, just to clarify?

Mr. GANNON. The national customer means the cabinet-level, Washington-based policymaker with the President, the White House, at the top and——

Chairman LIEBERMAN. As opposed to the——

Mr. GANNON. As opposed to the warfighter, the military establishment. So if I have a request for analytic support say at that time, from CINCPAC, I would probably respond with something like, "Well, if you could wait a few days, I will get a sanitized version of the product to you." I saw in the 1990s the environment change and the customer in the field became more demanding, partly because of the digital revolution—we actually could provide products in real time; and, second, because diplomats and military commanders abroad demanded that we do so. Admiral Dennis Blair, for example, was at CINCPAC, and he would say, "Heck, no, I need it now. Look at the challenges that I face"—this is the post-Cold War period. I have multiple threats in my AOR. I need to have real-time intelligence, and I need to have the best that you are giving to the President."

So what we saw then was a decentralization of intelligence support—CIA was less "central" and other agencies and sources of information played larger roles.

In the prolonged Balkans conflict, we saw the demand was not only to get information out there in realtime, but to actually have intelligence capability in place in the field where folks there could levy intelligence requirements and get a timely, tailored response. That is what I was talking about with reference to the JSOC model in Afghanistan or about what Mike Hayden and I meant by the IC's networked environment. So my point is that I think we can sort of lighten up about how much we want a DNI to control. The distributed or networked system is working very well, and a DNI should be nurturing at a strategic level, not trying to control it at a tactical level. He should be looking for gaps to close to better enable it, to better resource it, and to grow capabilities for the intelligence. But I do not think there is any way we are going to get

back to the old days when you had a centrally controlled system of intelligence support.

Chairman LIEBERMAN. Right. And I hear you saying that we should not try to get back to that, but——

Mr. GANNON. No. It is just a question of——

Chairman LIEBERMAN [continuing]. The world has gone beyond that.

Mr. GANNON. I think you can have a very successful authoritative DNI who is not worried about central control. By the way, I do not actually see a Secretary of Defense who has to worry about a lot of what goes on beneath them. A lot of the success we have had in Afghanistan and Iraq is because we have developed a distributed system of intelligence support, and that means we should not have an intrusive central authority getting in the way.

Chairman LIEBERMAN. That is great. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

We have talked a lot about the DNI this afternoon. I want to get your assessment of the National Counterterrorism Center. I remember when President Bush, by Executive Order, created what was then called TTIC. It was the predecessor agency of NCTC, and I visited—I believe that Senator Lieberman was with me. I visited TTIC and I remember being struck by how young the analysts were and got the distinct impression that agencies sent over their least experienced analysts to the TTIC. By contrast, when we visited NCTC, the analysts seemed to be far more experienced, and there seemed to be competition to be assigned to the NCTC. Totally different.

But that is my observation as a Senator. I would like to hear your views of NCTC. Has it been effective? Where does it need to go? And I will start with you, Mr. Gannon.

Mr. GANNON. I think NCTC has been effective. I think it has grown from strength to strength. I think it is much better today than it was 2 or 3 years ago. I think it is doing a commendable job of integrating foreign and domestic intelligence and producing analysis for a much broader, really nationally based customer set.

One issue which I think needs to be addressed by leadership—and I think it is a leadership issue—is the tension between NCTC and the CTC at CIA. I was actually around in 1986 when we created CTC. CTC and NCTC have different, equally valuable missions, and I do not think it is that difficult to appreciate. They need to support one another, but CTC is geared toward support for operations in the field, while NCTC has a mission to integrate foreign and domestic intelligence for the U.S. Government as a whole. It is not an intelligence collection or operations organization. Its primary role is analalytical.

I think what has happened is that the CTC in the Washington domain is getting less recognition, less respect. I believe it deserves a tremendous amount of credit for what it has been able to do in providing analytic support to operations. I think the reputation it has in the field, if you talk to special operations people, for example, is very powerful. I do not think it has ever done better than it is doing now. So why would we want to see that organization in any way diminished because we have created a NCTC? I think you can have both of them and be glad for it.

The rap against the CTC has been that it provides analysis in support of operations; it provides less direct support to the Washington community. Now we have the NCTC that can do that and does it well. NCTC has the responsibility that CTC does not have to do the integration of foreign and domestic intelligence. There has to be appreciation in the White House and in the Congress that there are distinct missions here, that both these organizations do well and their people have to be given credit for what they do. And my perception is that CTC is not getting the credit in the Washington environment that I think it deserves.

Senator COLLINS. Thank you. General Hayden.

General HAYDEN. Very briefly, I agree with everything that Mr. Gannon just said. I was asked this question in both the DNI role, Deputy, and head of CIA. What is the division of labor between the two? And one thought that is quickly tossed out but it is wrong is strategic and tactical. It is not. And what I am going to tell you now is not perfect. It is blurry. But I think as Mr. Gannon suggested, that is OK. It is a bit offense and defense. You turn to the NCTC first to deal with threats to the homeland and what needs to be done about it; hence, the more powerful blending of foreign and domestic intelligence and law enforcement.

The CTC has its center of gravity on the offense. We are going after these people. We need to know where they are. And so I think we are blessed to have both. We are lucky to live in a Nation that has the resources that it can afford a little—I will call it "redundancy," not duplication, or competitive analysis. But, fundamentally, they are different and they are focused on different things.

Senator COLLINS. Thank you. Representative Harman.

Ms. HARMAN. The Terrorist Threat Integration Center—yes, I know.

Senator COLLINS. You remembered.

Ms. HARMAN. I remembered. It was set up by President Bush I think out of frustration that the intelligence function of the Department of Homeland Security was taking so long to be established. And I think TTIC, which has now become the National Counterterrorism Center under our 2004 law, has served us extremely well. I understand this point, but I think our big threat now is attacks to our homeland, and the piece of this we need to nurture—and, in fact, it is doing well—is the NCTC.

It is very ably led by Mike Leiter, who is a holdover from the Bush Administration, a very good call by President Obama to keep him there, and it along with something called the ITACG—it is a group of police and first responders who come to Washington for a year and work at the NCTC—is preparing good product for local law enforcement so they know what to look for and what to do. NCTC plays an indispensable role in that regard.

The other point I would make is that after the Abdulmutallab plot was finally foiled—that was not a great moment for our intelligence community—Mike Leiter set up something called "pursuit teams." He discovered that there was no one in the U.S. intelligence community who had sole responsibility for detecting and piecing together disparate threat information. Talk about offense-defense. That is an offense we absolutely need in order to protect

our homeland, and NCTC provides that. So I think we have room for both of these things.

I think the weak actor in this picture is still the intelligence and analysis function at the Department of Homeland Security. In the Bush Administration, Charlie Allen had that job, and he was the legendary CIA Director of Operations who built, in my view, a kind of mini-CIA at DHS. I am not sure we needed it there, but I surely think we need more than what we now have there. In fact, it is kind of telling that Rand Beers, who is not the Director of I&A but is an Under Secretary of Homeland Security, has the portfolio for counterterrorism at the Department of Homeland Security, not the Director of Intelligence and Analysis.

Senator COLLINS. Thank you.

Is there any recommendation that you would like to make to us as we look to revise, if necessary, the 2004 Intelligence Reform Act? Mr. Gannon.

Mr. GANNON. Well, I think we are in a period of transition in the leadership in the intelligence community, and this would be a great time, I think, to take a step back and talk with people who have been or still are in the saddle. Robert Gates is leaving. There is nobody who has more knowledge and more desire to make things work. He knows both the intelligence and defense communities intimately. I think Jim Clapper is a man who works very hard to collaborate work with others. I cannot imagine having a better DNI for the times we are in.

So I'd suggest that you bring some of the folks who are leaving, have left, or are still in office, to talk about how best to proceed from where we are. Mr. Hayden is an example. Let us admit that we have the need to make the DNI position work. Let us recognize that we have a terrific guy in Jim Clapper and a very capable set of leaders today across the intelligence community. They all can help to drive us forward in a constructive direction.

Senator COLLINS. Good idea. Thank you. General Hayden.

General HAYDEN. I would be receptive to whatever the DNI brought you when he needs changes in law to go where he has to go. I do not think they will be numerous, but when they come, I think you can bet he needs them to get from here to there.

But to echo what has been said at the table before, it is a lot more dependent on the individuals and taking full advantage of the law, and those informal structures that get so much done in such a complex kind of organization. And so I would keep a close watch on that, and if you do end up with, for want of a better word, pathologies in terms of process or personalities, then there is not enough history and there is not enough structure to overcome that. And, therefore, that is a danger sign of which we need to be aware.

Senator COLLINS. Thank you. Representative Harman.

Ms. HARMAN. I think the law is a good law, and it is working, and the people in the top positions are excellent. And we had an enormous success last week, and we have had other substantial successes over the last several years. We are getting better and better at this, building on the record of three administrations. The pursuit of Osama bin Laden started under the Clinton Administration when he was indicted, and a unit at the CIA was set up to pursue him. We did not get very far with that. The then-National

Security Advisor's hair was on fire, but, alas, we did not get the job done. And through the Bush Administration and now the Obama Administration, with success of congresses, we are doing better. So I would kind of say that is in good shape.

A piece of the law that has never really been implemented is the formation of a robust Privacy and Civil Liberties Board. I know both of you have written letters. In my last job I wrote letters. Two people at the top have now been designated by this Administration, but I do not think the board is filled out, and I am quite sure it does not function. And why does this matter? It is not just to check a box so the civil liberties community, which is a robust community, and should be, is happy. It is to make certain that there is full vetting of policies that affect our U.S. Constitution and the implementation of the FISA amendments that we all worked so hard on and the implementation of the Patriot Act, and perhaps new policies to deal with something I know you are both worried about, which is our vulnerability to cyber attacks.

We want a group of knowledgeable people to screen these things and then to persuade an anxious public that the policies are a good idea. I was told today that the Patriot Act extension may be in trouble on the Hill in both parties because people do not understand why we need it. I think they would understand that better if there were a bipartisan Privacy and Civil Liberties Board to explain this.

And the final point is that our vulnerability in the near-term future is to our homeland, and that is why the NCTC matters, and that is why vertical information sharing matters. We have to think very carefully about the domestic intelligence space and how we are going to move forward and make sure that we do not trade off liberty for security. I do not think that is a zero sum game. I think we will either have both or we will have neither. And getting from here to there will depend on the watchdog that the three of us plus Pete Hoekstra insisted be in the 2004 law that has not yet been fully operational.

Senator COLLINS. Thank you all. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins.

Just one more item that I want to take up with you while we have you here. My impression from the testimony, at least of Representative Harman and Mr. Gannon—using a term, General Hayden, that you used, "unity of effort"—is that we do not have the unity of effort regarding domestic intelligence that we have regarding foreign intelligence.

I know, Representative Harman, you have been critical—or you said Intelligence and Analysis at the Department of Homeland Security is not where it should be. I agree. I think Secretary Janet Napolitano is working on that, and they are getting better. But I wanted to invite any of you—and we will start with Mr. Gannon because you made this point. What is the problem in terms of unity of effort? You were not criticizing the FBI. You were admiring the improvements they have made in their counterterrorism. But what do we need to do? And does the DNI need additional authority or, again, is this one of those areas, as you said before, that the DNI, looking across the community, maybe this is an area that the DNI

with the authority he has now ought to focus in on to make sure it works better?

Mr. GANNON. I will make several points. I think you are dealing in the domestic arena with, frankly, new agencies, like the Department of Homeland Security. If you compare it to the Department of Defense or CIA, they have years of working on the foreign intelligence side and developing capabilities that are quite extraordinary. We do not have those capabilities domestically.

On the FBI, I would actually have some criticism for where the Bureau is today. But I would also say that we underestimated the difficulty of transforming a law enforcement agency into an intelligence agency. If I had been at the CIA and they told me to transform it into a law enforcement agency, I would have been horrified. So I think we had to expect it was going to take some time.

And then some of the constituent agencies of the Department of Homeland Security, they are doing their own thing, but they are also dealing with new missions. There is a lot of overlap in the perceived missions of domestic agencies. But I would also say that we have fragmented congressional jurisdiction that I think has been a real problem. There is not what I would call the "adult supervision" needed to encourage all these agencies to develop a common strategy, to establish clear roles and responsibilities, and then to measure their progress against the strategy.

Chairman LIEBERMAN. The adult supervision from Congress.

Mr. GANNON. Yes.

Chairman LIEBERMAN. Yes. You are not calling us childish, are you? No, I know what you mean.

Mr. GANNON. I was not talking about you.

Chairman LIEBERMAN. I know. [Laughter.]

This is the most significant failure that we had in working to adopt the recommendations of the 9/11 Commission. We were really pretty good at reforming the Executive Branch, but when it came to reforming Congress, it just did not work.

Mr. GANNON. On the national side, you have the CIA with years of practice with counterterrorism to bring forces together. You have JSOC now in the field, which really has become a focal point for driving intelligence collection and anlayses. There is no comparable gravitational pull on the domestic agencies to work collaboratively.

Chairman LIEBERMAN. Right, and as you said in your testimony, there is nothing like that.

Mr. GANNON. You do not have any counterpart on the domestic side, and a lot of what is being done, including with the FBI, is a work in progress. I do not see an agressive or effective approach on the part of the Congress to really put quality measurement on what is going on.

Chairman LIEBERMAN. So what should be done about this? General Hayden.

General HAYDEN. Well, first of all, let me just say I agree totally with everything that Mr. Gannon has just described. It is not bad people or lack of effort. This is very hard for us to do because we have not done it historically.

Chairman LIEBERMAN. Right.

General HAYDEN. I recall your legislation sets up the FBI to be, in essence, a domestic intelligence service.

Chairman LIEBERMAN. Correct.

General HAYDEN. And everyone says that is great in 2004, and in late 2008, Attorney General Michael Mukasey finally issues the FBI guidelines with regard to working the spaces between cases as a domestic intelligence service, and you saw how well that fit inside the popular political culture. It just unleashed a firestorm of criticism. So this is hard because we have not done it before and our political culture has a bit of a rejection for it.

It brings us to the point that Congresswoman Harman brought up. You make people feel better if you have those mechanisms in place and working. You give a comfort level that this is being overseen as well.

I guess to reinforce it, this is a very important if not the most important area of focus. The new flavor of threat—homegrown, low threshold, self-radicalized, individual—puts a lot more weight on domestic as opposed to foreign and a lot more weight on law enforcement derived as opposed to intelligence derived. And if we do not begin to perfect our processes and organizations there, something bad will happen, and we will overreact and perhaps make it even worse.

Chairman LIEBERMAN. Yes. Well said.

Go ahead, Representative Harman. I was going to ask you if you agree with what has been said and, if you do, whether this is a matter of trying to give new authority again to the DNI or just urging the DNI to focus in on domestic intelligence as one of the weaker links in our chain.

Ms. HARMAN. I think the DNI has adequate authority. I think we need to have—and this is something you can do—a public debate about how to do this, not whether to do this. I think most people get it that the risk of homegrown terror is great. Maybe the harm from homegrown terror will not be as great as two towers in New York falling down and killing 3,000 people, but it is certainly possible—we all know this—that nuclear or radiological materials not only can be smuggled into this country, but certainly the radiological materials are already here and could be assembled into a dirty bomb, or several, and harm a lot of folks.

But my point is that we need public buy-in. It is not just making people feel better, Mr. Hayden. At least that is my view. It is making them agree that our Constitution will be respected, and it must be; otherwise, the underpinnings of our country are gone, and we turn into something else, which I surely do not want us to do.

We have not yet had a robust public debate about a comprehensive framework, new security framework in a post-9/11 world. We have done it episodically. We amended the Patriot Act, which I supported. We did FISA amendments. We did surely intelligence reform. But we have not thought through how all the pieces fit together, and I do not know that we would agree, and I do not know that this is the best time for Congress to do this since there is an excess amount of partisanship in Congress at the moment. But if ever there was a time to give this Committee adequate jurisdiction to hold that debate and do broader legislation, not just moving boxes around for the DNI but really thinking about in a new world with 21st Century threats how should Americans living our values deal with detention, interrogation, and investigation of Americans

on American soil; racial profiling or other activities that are anathema to some people; and how should we do this comprehensively. I think this is the time, and this is a huge service you could perform. I think the hearings you are holding right now are very helpful, and I am very happy to participate in one.

But I would urge the Congress to play its role as a co-equal branch of government—Congress writes the laws—and to thoroughly assess what is the right way with public buy-in to fill this domestic intelligence space.

Chairman LIEBERMAN. Thank you. That is an interesting place for us to come, but it does point to a kind of top of what needs to be done next, and it does relate, as you all have said, to the unique threat, which is to say we did not have homegrown domestic terrorism in our mind when we adopted the 2004 act. It now becomes a very significant part of the threat that we face, and we are trying to do this in ways that are different, as you all said.

For instance, DHS is trying to interact with State and local law enforcement, literally hundreds of thousands of people. I mean, they are obviously interacting with the leadership, but it is potentially a mighty force of gatherers of intelligence if you can do this well. And we are still feeling our way.

I do not have any more questions. Senator Collins, do you?

Senator COLLINS. No. Thank you.

Chairman LIEBERMAN. I want to thank the three of you. It has been a very valuable session for us. You have really brought to bear the quite remarkable and long experience that you have all had, and we are going to continue these hearings and then step back and decide whether we think there is any legislation to propose in this session of Congress to better achieve the purposes for which the original legislation was adopted or whether this is a matter where we ought to just agree on a report or even—in part public and in part maybe just to meet with some of the key players and say we have taken a look at this, and here is what we really think based on our inquiry you ought to be focused on now. It does not require a new law, but it does require attention and coordination.

With that, I thank you. The record of the hearing will stay open for 15 days for any additional questions and statements.

The hearing is adjourned.

[Whereupon, at 4:15 p.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11: IS INTELLIGENCE REFORM WORKING? PART II

THURSDAY, MAY 19, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 1:33 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Carper, Collins, and Brown.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good afternoon. This is our second hearing on the topic "Ten Years After 9/11: Is Intelligence Reform Working?" This is part of a continuing series of hearings that our Committee is convening this year on how well the security reforms enacted after 9/11 have protected our homeland, obviously with an eye on the 10th anniversary of 9/11 coming up.

During our hearing last week, we explored a variety of issues related to intelligence reform. This hearing is really going to focus on a single big question, but with a lot of sub-questions, and that is, does the Director of National Intelligence have the authority needed to lead our sprawling intelligence community as we want it to be led?

We are very honored to have with us as our sole witness today the immediate past Director of National Intelligence, Admiral Dennis Blair.

Admiral Blair is an extraordinarily talented and dedicated public servant who has had an exemplary career as a senior military commander and, of course, as a continuing consumer of intelligence before he overtook its production in one of Washington's, I would say, most challenging jobs—the Director of National Intelligence. Therefore, he is uniquely qualified to help us answer the questions we have about how the DNI has performed, and his willingness to testify I think is in keeping with Admiral Blair's lifetime of service to our country. So I thank you for being here today.

This Committee created the DNI as part of the Intelligence Reform and Terrorism Prevention Act of 2004 at the recommendation of the 9/11 Commission, which concluded that basically no one was in charge of the U.S. intelligence community, and that this lack of leadership resulted in dysfunction and disunity that left us vulnerable to the attacks that occurred on 9/11.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00075 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

The nature of the threat has changed certainly from the post-Second World War period and the Cold War, and even since 9/11 with the dispersion, in a way the metastasizing of the Islamist terrorist movement and also the development, for instance, of a very serious cyber threat to our security.

In the midst of all that, our intention was that the DNI would bring the necessary unity of command and effort to our 16 intelligence agencies.

So we come together today to ask: On a day-to-day basis, does the DNI have the authorities needed to lead the intelligence community effectively? Does the DNI have the ability to forge the unity of effort across the community and achieve the level of integration that is necessary to meet the range of security challenges that our Nation faces and the range of needs for intelligence that various people in our government have?

These are the overarching questions that I hope we will have the opportunity to pose to Admiral Blair today.

With that, I am going to put the rest of my opening statement in the record [1] and call on Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

The operation that tracked and killed Osama bin Laden demonstrates the kind of successful collaboration between our intelligence and operational capacities that we envisioned when we reformed our intelligence community in the wake of the attacks on our country on 9/11.

This was undoubtedly a great victory for our intelligence efforts and a great blow to al-Qaeda. But the fact remains that al-Qaeda and other terrorist threats are not going away.

That is why it is time for Congress to examine and build upon the successes since the Intelligence Reform and Terrorism Prevention Act was passed. That bill created the Director of National Intelligence. It is an opportune time to identify any shortcomings in that structure and work to correct them.

I look forward to hearing from Admiral Blair about what worked during his tenure as DNI, what did not work, and what might be changed about the structure that we designed 7 years ago.

I would note with great pride that Admiral Blair is a fellow Mainer—hailing from Kittery, Maine, the home of the Portsmouth Naval Shipyard. So either coming from a great Navy town or following five generations of naval officers perhaps preordained his career. We all hope that he has what we call a great Navy Day here as we hear from him about his experiences as the DNI as well as his recommendations now with the benefit of actual experience and 20/20 hindsight.

Almost 10 years since September 11, 2001, and 7 years since our landmark legislation, we are safer as a Nation but not yet safe. Our intelligence community is stronger and more effective than ever before, but plenty of turf battles remain. During his tenure Admiral Blair was at the center of some unusually public disputes with the CIA.

[1] The prepared statement of Senator Lieberman appears in the Appendix on page 412.

To help address lingering deficiencies in the intelligence community, the DNI must be the "quarterback" that the 9/11 Commission envisioned and that we intended. At last week's hearing, General Hayden preferred the term "coach." I will be interested to hear whether or not Admiral Blair believes the DNI has been empowered to fill this critical role, regardless of what you call it.

At the first hearing in this series, the leaders of the 9/11 Commission, Governor Thomas Kean and Representative Lee Hamilton, agreed that presidential adviser John Brennan is, in many respects, performing the role that we envisioned for the DNI when we authored the law; that troubles me, not due to any doubts about Mr. Brennan's capabilities, but because that choice, that structure undermines the statutory role of the DNI.

We must ask, therefore, the fundamental question: Are changes in the law required in order to realize the potential of the DNI? Or is this simply a matter of more fidelity to the 2004 law?

Admiral Blair, thank you for being here today, and I look forward to hearing your testimony.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

Admiral Blair, it is all yours. Thanks for being here.

TESTIMONY OF HON. DENNIS C. BLAIR,[1] FORMER DIRECTOR OF NATIONAL INTELLIGENCE

Admiral BLAIR. Mr. Chairman and Senator Collins, thank you for inviting me here today. It is common to improve the effectiveness of government after some disaster or crisis, and, in fact, the Intelligence Reform and Terrorist Prevention Act of 2004 was born of 9/11, as you mentioned, Mr. Chairman. But I think that reform in the wake of success also has a history. Those who led the great victory of World War II knew that there were major improvements to be made in the national security organizations, and when the parades were over, they passed bold legislation to make the country safer.

So as we celebrate the brave, dogged, and brilliant work of those who found and attacked Osama bin Laden in his hideout, I believe that now is a similar time for bold laws to make this Nation's intelligence enterprise even more effective than it is.

And as I look to our future national security challenges and opportunities, I am absolutely convinced that we need an intelligence community that operates under authorities that are relevant to the future, not to the past, an intelligence community that is organized on a rational basis, and an intelligence community that is integrated under a strong and competent Director of National Intelligence.

I left the Administration a year ago frustrated with the lack of support for a strong DNI, but I was reluctant to appear publicly before this Committee where my comments could perhaps be miscast as sour grapes from the loser in some petty bureaucratic squabble. But I believe that the imperative of an integrated, effective intelligence community should transcend policy and politics and personalities. The country needs and deserves legislation that will establish the best intelligence capability possible, independent

[1] The prepared statement of Admiral Blair appears in the Appendix on page 416.

of officials and Administrations as they come and go. So let me use the rest of my introductory time to highlight the improvements that I believe are still needed.

The objective is to make the structure of the intelligence community worthy of its people, whether in the CIA, NSA, NGA, FBI, DEA, DIA, the service intelligence organizations, along with the other seven intelligence elements of our government. These heroes, these people who are in those organizations, are every bit as dedicated, patriotic, and skilled as the members of the armed forces and first responders whose heroism inspires us and makes us proud. We owe them integrated leadership. So let me run down areas where I think we can do more.

First, organization. Right now the Department of Defense and the intelligence community conduct operations together under separate authorities—Title 10 and Title 50. To be effective against dangerous, elusive, and quickly adversaries like al-Qaeda, drug cartels, outlaw States, a new title is needed authorizing joint interagency task forces that can bring to bear all the capabilities of both organizations under unified direction. We need a Title 60.

Right now the structure of the Central Intelligence Agency, one of the most important of the agencies, is a kludge of one organization that collects human intelligence and conducts covert operations and another organization that provides all sorts of intelligence analysis, of which the greatest proportion is, in fact, provided by the NSA, a different agency. But the skills, procedures, competencies, and cultures of these two sub-organizations are very different, and their collocation yields little synergy and has major disadvantages.

I recommend that the CIA be broken into an all-source analytical agency and a national clandestine service, each led by a career professional with a fixed term, each reporting separately to the Director of National Intelligence, and I recommend that some elements of the Defense Intelligence Agency performing all-source analysis on the one hand, human intelligence on the other hand, be added to those two new agencies.

Moving to authorities, current legislation and constitutional precedents have little application to the Information Age, and the efforts that I observe to adopt them have been completely unsuccessful. The National Security Agency has the world's best ability to provide protection for the country's Internet domains, yet it is not securing the important dot-gov domain, which your computers use here in the Congress, and the vital infrastructure, the dot-com domain.

An official responsible for cyber defense should be dual-hatted, reporting to both the Secretary of Homeland Security and the Director of NSA with the responsibility for bringing NSA's capabilities to bear to protect these vital systems.

Right now there is no legislation that clearly authorizes offensive cyber operations by the United States against enemies that use the Internet to threaten American lives and property. Extremist Web sites incite violence, provide practical bomb-making advice. International drug cartels use the Internet to arrange deliveries of drugs and to purchase weapons. Foreign outlaw nations are making cyber plans that threaten vital interests. Yet because often

these threats are carried out on American Internet servers or because there is a possibility of collateral damage from attack or because a hostile actor and illegal action has not yet occurred, the United States has no basis in current law for the sort of quick, effective action that we need against these threats. The country needs such legislation. It should include limitations related to the proportionality of what is being done, related to avoiding collateral damage. It needs oversight mechanisms in both the Executive and the Legislative Branches. But it must provide a basis for action commensurate with the threat.

And, third, the authority of the DNI within the intelligence community. The intent of IRTPA was clear, and you have both stated it. I believe it was correct. The intelligence community needs a leader, an integrator not a coordinator. The intelligence community does not self-synchronize. Few organizations do. We learned that on 9/11. The White House has neither the staff nor the time to lead it, and it often approves misguided schemes, as this country has learned to its sorrow in past instances.

The authority that the Congress intended for the DNI to exercise is not now intact. Currently, a portion of it has migrated back to the Director of CIA on the one hand and some to the National Security Council staff on the other hand. The result is a confusion of responsibilities, bureaucratic fiction, but, more important, potential gaps in intelligence that our adversaries can exploit.

There are several legislative changes that I believe can strengthen the authority and the accountability of the DNI.

First, personnel. In addition to naming or concurring with the appointments of the heads of the intelligence elements currently provided in IRTPA, the DNI should approve the appointments of second- and third-level officials within the intelligence elements. This authority will ensure that community-minded officers occupy the important posts where much of the real work of intelligence is done.

Second, budget. The DNI's budget authorities in practice are strong in future budget years but relatively weak in the current fiscal year. He or she should have the authority to initiate reprogramming of funding from agency budgets to urgent and emerging unexpected objectives, for example, network security against new threats, or simply to higher-priority objectives or simply to programs that are not making the progress they should.

So, in conclusion, Mr. Chairman and Ranking Member Senator Collins, the success against Osama bin Laden should not cause us to rest on our laurels. We are a long way from an integrated intelligence community smoothly interacting with the Department of Defense, the Department of Homeland Security, with integration being driven by a strong DNI and a competent staff, and I believe congressional action is indispensable to this goal.

The reform of our intelligence community is an unfinished, vital piece of business. I find it reassuring that you see fit to keep this challenge alive and take seriously the progress we need to make, and I am happy to answer your questions.

Chairman LIEBERMAN. Thank you very much, Admiral. I appreciate what you said at the beginning, but honestly, no one listening to your statement or reading it could think you were here out of

some sort of personal pique. The fact is we asked you, and the second is, listening to your statement, it is totally substantive, and truly it is exactly why we asked you because you are part of a very small group of people who have actually been the DNI. So you have that perspective, and obviously you bring to it everything else you have done in your career.

We are going to do 7-minute rounds of questions.

Let me ask you this question to begin with. It touches somewhat on something Senator Collins said. In the testimony last week, I was fascinated that at different points our witnesses—who were Jane Harman, General Hayden, and John Gannon—suggested that it may be as critical to accepting the goal of the strength and legitimacy of the DNI for there to be adequate support from the President—and to a somewhat lesser extent Congress in a different way—as it is to add on to the statutory authorities of the DNI. And I wonder what you think about that. It may not be an either/or question, but give me your sense of how important the non-statutory recognition and authority given for the office is.

Admiral BLAIR. Senator Lieberman, I would agree with that observation that active support from the White House and the Congress makes it a lot easier for a director to fill in the gaps of authority in legislation, and that would be a good thing. However, I do not think that is a reason for the Congress not to continue to strengthen the intelligence community integration in a way that I think IRTPA was designed to do because as I mentioned, Administrations and personalities come and go, but it seems to me it is the responsibility of the legislation to establish that structure right in accordance with what we have learned over time.

I think what we have learned over time—and this is not the only time that the Congress has attempted to integrate related but not really cooperating agencies. The National Security legislation of 1947 which brought the services together based on the results of World War II, the Goldwater-Nichols Act of 1986, the creation of the Department of Homeland Security—these things are always difficult to bring in children who think they are happy into an orphanage. That does not always go easily. But it takes persistence, and it takes a dedication to believing that this is the right thing. And I think Congress has a role.

Right now there are two models of an intelligence community that we have seen in the last 5 years. One is one in which the Director of National Intelligence is expected to be able to integrate the community and to be responsible for that; another in which that authority is sort of spread around among people, and the White House picks and chooses what it will use.

I think right now we see the model going toward that second model, which the group that is in the Executive Branch now believes. I think the first model is more correct, and I think that is what the Congress intended, and we need to continue to push that. And I think that 5 years into the DNI we had that—well, we are actually 6 years now. We are making good progress, and we need to continue to ring that out.

Chairman LIEBERMAN. Good. Let me talk about some of the authorities that the DNI has and how they might be expanded, and

then later on I would like to come back to some of your very interesting suggestions.

The 2004 legislation gave budget authority to the DNI, and that authority includes having the final say over the intelligence community budget that is presented to the President; also certain authorities called, as you know, budget allocation and apportionment authorities related to how the intelligence community spends its budget during the fiscal year.

In your prepared testimony, you called for the DNI to have increased "comptrollership" authorities so that agencies under the DNI could not seek to circumvent the DNI on budget issues. I want to ask how strong the authorities that the DNI has had over the budget have been in practice, at least certainly during your period of time, and whether you think the DNI has fully utilized those authorities over both budget development for future fiscal years and resource transfers during a fiscal year.

Admiral BLAIR. Yes, sir, Senator Lieberman. I think there are two important background points. Firt, is the last 10 years have been a time of rising budgets for the intelligence community just as they have been for the Department of Defense. So the tough budget trade-offs have generally been taken care of by putting more money on them rather than by reprioritization. I think those times are coming to an end, and we will see budgets that are flat and perhaps even decreasing, and that will make this central ability to make trade-offs even more important.

The second item was that just due to the number of tasks that faced the DNI early on, there was not a strong staff support structure for budget trade-offs. The equivalent of my experience was in the Department of Defense, the Program Analysis and Evaluation Office, the strong Comptroller at the Office of the Secretary of Defense had not been established. Those were coming into maturity while I was DNI, and I spent a great deal of time trying to strengthen them.

So I found that I finally, toward the end of my time, had the tools to use the budget authorities, and let me give you two examples of the kind of things I am talking about, because they came up during my final months in the job.

I came back from a trip to Afghanistan horrified by the lack of language ability that we had among our deployed officers in that country. I will not give you the numbers, but the number of Pashtu and Dari speakers was smaller than I thought was safe.

As you know, language ability was in IRTPA from the beginning, and the agencies have been chugging along—it was time to say, "all right, now, and we are going to move the money in, we are going to make it happen." That is the thing that I am talking about where well-meaning agencies were making their own priorities, that sort of allowed a national priority to drift down, and you needed to be able to punch it.

Chairman LIEBERMAN. Were you able to do that at that point with the authorities you have?

Admiral BLAIR. At that point, we had the "Come to mother" conversation, and I was going to give them one more chance to do it themselves before I did it, and then I left. So that is where it stood.

Chairman LIEBERMAN. But you felt that you had the authority to carry that out if you needed it.

Admiral BLAIR. I was going to find out. [Laughter.]

That would have been the first one.

Chairman LIEBERMAN. Well, you were right, of course.

Admiral BLAIR. And, I mean, the usual thing that I saw was what happened after the Detroit bombing in December 2009 by Umar Farouk Abdulmutallab. We had obvious problems in the search engines that were available to counterintelligence analyst that required banks of computers, different skills on different systems. And as you saw from the final reports, we missed some of those, and part of it was due to an analyst not being able to hit just one click to make a query and have the answer come back. It required a lot of skill, which busy people often do not have everything they need. What happened is we received more money to fix that problem, and my job was only to spread it out.

Now, there were fairly decent battles on how to spread it out, and, each agency said, "I am the one who ought to get the lion's share, and I do the work," and so on. But those are different problems from going in and carving it out and putting it on the thing, which is what I was talking about in terms of real comptrollership in which I was used to the Secretary of Defense's Comptroller being able to do routinely in the year of execution. So that is really what I am talking about in a sense.

Chairman LIEBERMAN. Understood. Well said. My time is up. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Admiral Blair, you were just talking about Abdulmutallab and some of the problems that were exposed by that intelligence failure. I am curious. Were you consulted by the Attorney General on the decision to charge Abdulmutallab as if he were a criminal suspect?

Admiral BLAIR. I was not consulted on that particular decision, Senator Collins, nor do I think I would have had much to add. I think the key role that the Director of National Intelligence plays is during the questioning phase of a suspect once apprehended or arrested. How much do we lean on intelligence gathering and how much do we lean on gathering material for prosecution which involves sort of a different set of protocols? And the most famous one that everybody talks about is the reading of Miranda rights and the provision of a lawyer and so on.

On Abdulmutallab, I was not consulted on that either. As you all know from the hearing that we held here, that set of decisions was made by the agents at the scene, and it was not really supervised, and we did not have the High-Value Interrogation Group stood up well enough to be able to take that. But I believe strongly that is the point at which the Director of National Intelligence or his representative should make an input, and the goal is to be able to do both so that the Attorney General can make a decision: Military tribunal, Federal court, or nothing.

If you have to make a trade-off, that is when you need to say, we are drilling ahead to get intelligence information, and we are going to back off on perhaps gathering evidence. And I think that is what I should be involved in.

Senator COLLINS. I realize that we had gone through that issue before, but the reason that I brought it up again is I want to lay the predicate for my next question, which is: What is the role of the DNI when a terrorist suspect is apprehended? It seems to me that one of the first calls, if it is a surprise apprehension, should be to the DNI so that a search can be done immediately of all databases so that intelligence analysts and the HIG—which is now, I believe, set up—could be flown out to wherever they need to go. But I want to hear from you more what you see as the role. You were starting to get into that. I was not trying to relive who told what but, rather, for those who were not around when we explored that before, I wanted to lay the predicate.

Admiral BLAIR. Yes, ma'am. The theme you will see throughout all of my testimony and my thinking that I have become passionately to believe is that we need to be able to quickly bring together the skills of anybody in government and many from outside of government who can apply their skill to it.

So let us say that we on a surprise apprehend a member of al-Qaeda in the Arabian Peninsula. We should be able to get the best intelligence Yemen analysts, the best counterterrorist analysts and at the same time the best FBI interrogators, the best people in the FBI who have been working terrorism. There should be a structured process that they have a quick conversation. The different equities and the different approaches are laid out on the table. We have a decisionmaking process so that a call can be made in terms of that balance. And then under tremendous time pressures—minutes, hours at the most—the people on the scene go ahead and proceed in accordance with that guidance. And you have to have practiced it some first. These people cannot meet each other the first time when it is a real situation. And it is really setting up those procedures that can do it.

My experience is that we have such good people across the board in law enforcement and the intelligence community that with general guidance from the top they can do the job perfectly. But there are certain key questions, and you hit a real one, the balance between gathering evidence and gathering intelligence, that need to be made at the top when there is a conflict. And I think in the case of Abdulmutallab, I think we had all the evidence that this guy had a bomb, tried to blow it up, which is all we needed. We did not need a lot of self-incrimination in that category, and probably we should have leaned harder on intelligence throughout than we did, because we pretty much had a Federal conviction, I thought.

So that is the kind of decision you need to make, and you need quick, practiced procedures to do it.

Senator COLLINS. As I look at the DNI or, indeed, any position in Washington, there are really three levels of power: First is access to the President; second is authority over personnel; and third is control over the budget. And I would like to talk about those issues with you, starting with the personnel issue.

Part of our concept was to try to have a Goldwater-Nichols-like joint approach to service in the intelligence community, and I am sure it took the military an awful long time to embrace that. But now, at least from my outside perspective, the military really has largely embraced jointness.

Where are we in the intelligence community as far as having that kind of joint approach where personnel is shared among agencies and where your ability to advance in your career in the intelligence community depends on joint service?

Admiral BLAIR. Senator, I think your provisions of the IRTPA to that end were exactly right, and I think they are biting within the intelligence community. They are having effect. If I try to compare it to 5 years into the Goldwater-Nichols Act, I would say it is sort of comparable in terms of the effect it is having. And it will take more time, but two trends really encourage me.

First is, as I talk to people, the younger they are, the more they get it. Half of the heroes in the intelligence community joined after 9/11 for the right reasons, and they are naturally more prone to sharing. They do not carry all that baggage of bureaucratic prerogatives and all that we all grew up with, the past bureaucratic wars that we all thought were so important and which actually did not help the country much. And so as they age up and get into the jobs, I think the trends are good.

The second one is that in the field—and you all have taken many visits out there. You walk into an intelligence center in Afghanistan, in Iraq, in just about any place in the world, you find people from NGA, NSA, CIA, and the armed forces in there working. If somebody has a piece of information, he is expected to contribute. So they are growing up in this atmosphere, and, again, as they bring that back stateside, all we have to do, I think, is provide them a modicum of structure so that you are not rewarded for bad behavior. You do not have to forget all that stuff you learned in the field. You ought to bring it back and use it, and it will take over.

So I think we are headed in the right direction, but like you I am impatient at the scale. I mean, I thought we decided this. Let us get on with it.

I think the next generation, the generation that is right on the cusp of leadership within the agencies is going to be quite more joint-minded, and if we can get the structures right, they will fall into it. What you have to realize is that you can be proud of your own agency, you can say, "I am a CIA person," but you also need this pride in the team. You also need this pride in everybody doing well and you do well, too. And I think when you have not experienced it, you think the pride is a fixed amount. You know, if somebody else gets some, it subtracts some from what you have. And I think we found in the Armed Forces that both pride and effectiveness go up exponentially when you can sort of get over the hump of that jointness and working together. And I think we are headed that way, but the suggestion I made of putting special attention on second- and third-level people I think is of a piece with that and would just help it along.

Senator COLLINS. Thank you. I think your point about the generational change is absolutely right, and I think we are seeing that with the use of technology and networking and sharing of databases, too, because that is just what the next generation does naturally.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. The other thing I would add is that I hope that particularly since 9/11 people with-

in the intelligence community understand that they can come under great public, including congressional, criticism if in a look back it appears that one or another part of the community—including the military, but particularly the IC we are talking about—was not playing on the team, and as a result the team suffered, and therefore, they will suffer a kind of rebuke that perhaps they would not have at an earlier time.

Senator Brown, it is all yours.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. Thank you. I know the vote started, so I just have a couple of quick questions.

General Hayden testified last week that the IC needs to find the critical balance between freedom of action for the parts and the unity of the effort for the whole. Is that balance achievable, do you think, given the current structure of the IC? And in what ways can the relationship between the DNI and the heads of the 16 intelligence agencies be improved or strengthened?

Admiral BLAIR. Senator, freedom of action, and what was the other pole of that dilemma?

Senator BROWN. The freedom of action for the parts and the unity of the effort as a whole. Is that balance achievable?

Admiral BLAIR. I think it is very much achievable, and what you find is in the best organizations that achieve that balance, people come in as an expert in their own field, but they are more than just sitting there waiting to say, well, if you want a piece of human intelligence, I will gather that for you. If you want a piece of signals intelligence, I will gather it for you. They come in with an attitude of being able to contribute what they can do, and based on their much better understanding of what other people's problems are and what the total mission is, how they can contribute in ways perhaps that are not traditional. And I have just seen that work time and time again. When you form these teams, you bring people into them with the attitude that everybody needs to contribute all they can and maybe more, and then magic happens in that interaction. I have seen it in terms of our teams in the intelligence community that can gather intelligence against very difficult targets by using our wondrous collection capabilities in new ways. I have seen it in action teams. I think one of the most poignant things I saw was I was off visiting one of our bases in a very dangerous part of the world, and a young CIA case officer told me a story that she had been on her way to a meeting in a restaurant with an asset to recruit. A complete other agency monitoring the situation had picked up a warning of danger. They had been able to get a phone call to her. She turned around, did not go to the restaurant, life saved, lesson learned. And it is that kind of teamwork in the field that I think becomes the norm when you create an atmosphere in which it is expected and it is valued.

Senator BROWN. Thank you. And I want to say thank you for your service, too, in your position. I wanted to just mention that first.

I know General Hayden testified last week that the creation of the Under Secretary of Defense for Intelligence, undermined Congress' attempt to strengthen the DNI because Secretary of Defense

Donald Rumsfeld delegated his authority, direction, and control of the major defense intelligence agencies to the USDI. Can you describe your relationship with Secretary of Defense Robert Gates and the USDI? And does the role of the USDI hinder the DNI's ability to exert his authority over the counteroperations or future directions of the entire IC?

Admiral BLAIR. That was not my experience, Senator Brown. I thought that General James Clapper as Under Secretary of Defense for Intelligence, and I, as DNI, worked very well together, and if he were sitting here, I am very confident he would say the same thing.

I know Senator Lieberman was involved in some of the angst from the Department when IRTPA was written. I found it largely to have dissipated by the time that I had the honor of being DNI.

I think there are two important reasons for this. First is the really important security challenges we face these days have so much of the military aspect mixed up with the non-military aspect—economic, social, others—that the idea that you can sort of hive off a military aspect of a problem and say, well, that is for the Pentagon, this other stuff is for CIA, INR, the civilian groups, is long gone.

If you look at our big problems—Afghanistan, terrorism, Iraq—the military aspects and the non-military aspects are all together, and you have to use your intelligence capabilities, whether they be signals intelligence, which happens to be collocated in DOD, or geospatial intelligence, which is sort of a hybrid, to look at the whole question. So we are driving toward this unity by just the nature of the problem.

Second, the officers or civilians in the case of Letitia Long, who is now the head of NGA, have grown up in this joint era that we were discussing earlier, and they understand the advantages of teamwork and the synergies that can come from that. I did not have any stronger teammates in community integration than Admiral Robert Murrett at NGA, General Keith Alexander at NSA, and General Ronald Burgess at DIA. That leadership was strong, and the USDI in my observation was part of the team, also.

So I did not see that, and I know it was the historical fault line, but it seems to have been helped. And, of course, Secretary Gates having had some piece of my job previously had a good understanding, and that helps, too.

Senator BROWN. Great. Well, thank you, sir. I appreciate it.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Brown.

Incidentally, for the record, General Clapper has said exactly the same thing to me about how good a working relationship he had with you. These are interesting comparisons because this is a case where I think the personalities that were in these positions under Secretary Rumsfeld and perhaps the Secretary himself were part of the problem, if I can call it that, and as you said, correctly, Secretary Gates comes to his position, after having spent most of his public service in the intelligence community. But you must have known General Clapper before, so you had knowledge of each other and just a willingness to work together, and you did to the Nation's benefit.

So it is interesting, as I have told you before, I think, Admiral, that during the legislative battles on the Intelligence Reform and Terrorist Prevention Act of 2004, the toughest ones were with the Defense Department about the changes we were trying to bring about strengthening DNI. And yet in practice, the tensions between the DNI and the DOD have been much less than were reflected at the legislative negotiating table. Without being specific at this moment, I would say that it was the opposite for other components of the IC.

So I really apologize for having to break the flow. The vote is going on on an important judicial nomination, so I am going to ask that we stand in recess, and I will be back as soon as I can to continue the questioning. Thank you.

[Recess.]

Chairman LIEBERMAN. The hearing will reconvene again.

Is that a new staff member? Oh, that is Senator Carper. [Laughter.]

Senator Carper, I can proceed with a round of questions, or I can call on you first, if you would like. It is up to you.

Senator CARPER. You are very kind. I would like to.

Chairman LIEBERMAN. Go right ahead because I have had one round. Again, I apologize, Admiral, for having to leave to vote. But I look forward to asking you some more questions.

Senator Carper, thanks very much for being here.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you. I do have a question. Welcome, Admiral. I am a retired Navy captain, so I salute you, in more ways than one.

I understand that today's intelligence reform hearing is focusing on whether the intelligence community is operating better, and if this question has already been asked, I apologize, but I am going to ask it anyway. And if you could respond, I would be grateful. But since the passage of the intelligence reform legislation in 2004, after the successful operation against Osama bin Laden—and as a Navy veteran of 23 years, I salute our SEALs and everybody who was part of that operation. I said to my colleagues today at another meeting that while I think there is a sense of justice with respect to Osama bin Laden and hopefully some closure for a lot of the families who lost their loved ones on 9/11 and other attacks, the greater benefit is, I hope, going to be our ability to use the intelligence that we recovered to better protect folks here in this country and other countries as well who might also be at risk.

But after the successful operation against Osama bin Laden and the thwarting of any number of terrorist attacks that were directed at our homeland and other places where we have interests during the last 9 years, I think that things are working better. I hope you do, too. I also believe we are in a safer place as a result of this reorganization that we put in place a number of years ago.

Specifically, I was impressed with, I think, last week's remarks by the Secretary of Homeland Security, Janet Napolitano, on how intelligence information from the raid on Osama bin Laden's compound was almost immediately being shared throughout our intelligence community. I am not sure this would have happened as

quickly or as smoothly before the work that has been done since 9/11. And while it is clear that institutional reorganizations are needed every now and then, without the President's national security leadership working together as a team, I think restructuring our Federal Government is only going to work partially.

Here is my question, and it really centers on the relationship between the President, Deputy National Security Adviser Denis McDonough, Assistant to the President for Homeland Security and Counterterrorism John Brennan, and Director of National Intelligence James Clapper—and whether the Director of National Intelligence will ever work as it was intended to with the first two positions being usually confidants in close physical proximity to the President than the rest of the Federal Government's national security leadership. Would you just think about that for a moment and maybe share some thoughts with us on that?

Admiral BLAIR. Yes, sir, Senator Carper. On the first observations you made, I agree completely. This was a very well done operation. What I think we need is to make that the norm, and I think it is understandable that we did well on that operation, the highest priority task that this Nation has had for the last 10 years in that area required deep personal involvement of the President, the high-level Cabinet officers themselves, and so on. So it is no surprise to me that we did well on that.

What I think we need to do is to get that same interaction and legislatively mandate that same interaction and teamwork in order to get everything done that the intelligence community, the Department of Defense, and the Department of Homeland Security are involved in. And I think we have made strides, but I think we have a ways to go.

On the question of the relationship between the DNI and the President versus his staff, this is what staff line relationships are all about. The President should get his advice from whoever he chooses to seek it from. He has staffers on his staff who are experts in defense, and I used to be on the national security staff as a commander in the Navy. Department of Homeland Security officers serve at the National Security Council staff. Outside experts are brought in. We all know how the advice of staff versus the responsibility of line officers should work, and I think that in the White House relationships with departments and with the intelligence community, just the same principles should apply. You should carry out your main actions and get the recommendations of those whom you appoint and whom the Senate confirms, and then you ought to use your staff to evaluate their recommendations and to check on how they are doing. And there will be tension between those two at times. You know, no good staff officer but thinks he can do a better job than this guy who has the job—until he occupies that job and wisdom occurs. So these tensions are natural, but I think the formal structure should be that those responsible officials at the right level should be carrying out the job and be held responsible for it.

Senator CARPER. Thanks. Mr. Chairman, do I have time for one more question?

Chairman LIEBERMAN. Go right ahead.

Senator CARPER. Thank you, sir.

I chair a subcommittee of this Committee that focuses on Federal financial management and a host of other areas. But one of the things that we try to do in the subcommittee, as the Chairman knows, is we try to look into every nook and cranny of the Federal Government and ask this question: Is it possible to get better results for less money, or is it possible to get better results for the same amount of money? We try to do that throughout the government. I sort of describe it as a culture change from a culture of spendthrift to more of a culture of thrift. It is a little bit like trying to turn an aircraft carrier. But we know if we try long enough and hard enough, we can turn aircraft carriers. So we can maybe even change the culture here.

This Committee is really a great Committee to be on. Governmental affairs used to be almost our sole focus, and how to make the government work to get better results for less money. And now we have this other hat that we wear in homeland security, which is terribly important, but we have not forgotten what our bread and butter used to be.

But a couple of weeks ago, I was returning from South Asia where I had been to, among other places, Pakistan, Afghanistan, and India, reviewing our regional counterterrorism strategy in Pakistan. One of the glaring success stories that was brought to my attention was how our intelligence community analysts and military specialists, both men and women, and special operations men and women, were sitting side by side each other and analyzing intelligence information. And I was very impressed with the cohesion that I saw on the ground.

My question to you is simply that today whether this new approach is part of a broader counterterrorism strategy in the region? And then, second, are there lessons learned from your experiences that you can share with us that you would like to see our military and intelligence communities implement tactically?

Admiral BLAIR. Yes, Senator. I think what you saw is just as good as you said it was, and I think it is a result of 10 years of the same set of mid-level leaders in the intelligence agencies and in the Department of Defense, primarily special forces working together against al-Qaeda and its subordinates. These extraordinary leaders in all of these agencies and services have learned to cooperate at the local level.

I would say they do that right now with the tolerance of the leadership, in some cases with the active support of the leadership, but there is not a structure that they can fall into naturally or that new people will fall into naturally when the urgency and the passion that 9/11 caused passes.

So I recommended in my prepared testimony for this Committee that we form joint interagency task forces. Let us pick a place like Yemen where both military counterterrorism capabilities and intelligence community counterterrorism capabilities can be brought to bear. I would recommend forming a joint interagency task force. The boss of it could be, for example, a military officer and the deputy be an intelligence community professional or vice versa. I do not really much care, but they need to be qualified for the job and have experience and all of the tools. And then instead of this extraordinary cooperation which now occurs, you can have a unified

effort in which the task force commander, after he has submitted a plan, has the authorities and can choose to use intelligence assets one way or military assets, and put them together, because what we found in our joint task forces in the Armed Forces is that you come up with new ideas when you put people together in one space with one mission, with a set of core competencies that are pretty extraordinary. They find different ways to do it. "Oh, that is what you need? That is easy. We can help you out with that. Why don't we try this?"

That sort of synergy comes much better by putting them together under one boss than it does by sitting there in their individual stovepipes, and with all the best will in the world and if the right people happen to be there, you can work out some of this stuff. But it is not institutionalized. The incentives are not right. The rewards are not right. There is a certain danger in cooperating. And so I vote for counterterrorism joint interagency task forces pointed at the key areas where we still face al-Qaeda and its affiliates.

Senator CARPER. Thank you so much for your responses and for that analysis. Thanks so much. Thanks for joining us today.

Thanks, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Carper.

Admiral Blair, let me approach the topic we have been talking about by sharing this analysis of our 2004 legislation, which is that it gave the DNI two major responsibilities: One was to be the leader of the intelligence community, and the second was to be the senior adviser on intelligence matters to the President. And I wanted to ask you both from what you know of your predecessors' and successors' experience and your own, one, just in terms of responsibility whether that is too much to ask of one person. Maybe I should leave it at that. But the second is a bit inconsistent with the first, in some ways following Senator Carper's question. Is it necessary for the DNI to be the senior intelligence adviser to the President in order for the DNI to have the credibility to be the leader of the intelligence community? Two different questions related to that same dual responsibility.

Admiral BLAIR. Yes, sir. I think that the DNI can and should have both those responsibilities. I do not think the DNI can have the additional responsibility of directing the CIA. I mean, that was the hand that we dealt the DCI, as you will recall.

Chairman LIEBERMAN. Right.

Admiral BLAIR. And integrating the community and advising the President, and I think it was extremely wise to cut those two off. But I also think that it is essential that leading the community and advising the President be combined in one person so that the advice can be realistic in terms of what it is the community can do, one; and, two, so that the Director, seeing the sorts of information the President needs, can turn around and say, "Listen, we have got to work harder on Problem X. I see this one coming. It is important to the President. We are not there yet. Do it."

Sometimes people forget that the intelligence successes of today are due to a lot of work done over the last several years, really hard work of collection, integration, spending money in the right place, language capabilities, and personnel assignments. And unless you are the person who ensures that all of that happens well

and direct some of it if it is not being done very well, you are not in a position really to tell the President how good the stuff that you are telling him is; otherwise, you are just taking some report from some analyst and parroting it to him, and you might as well have the analyst tell him directly.

So I think this combination of being the one who has the responsibility for making the intelligence good and then passing it to the President is important. I found it was often as important to tell the President what we did not know and why we did not know it than telling him what we knew because making high-level decisions under conditions of uncertainty is what we really pay the President for. Sometimes I would tell the President, "If I were perfect in intelligence, your job would not be very difficult. You would just ask me what is going to happen and choose the obvious course of action."

But it is that interaction of what the big intelligence machine can actually do, the burn that you need to do better so that when the President turns to you in a year and says, "What is the situation with nuclear weapons in Country X?" You have a good answer. That is essential to the DNI. So I do not think those two responsibilities can split up.

And, finally, the DNI should have the political sense of what is important to the President over the long term. President Grant knew that he had to win a battle before the Emancipation Proclamation could come out, and so he won one. I mean, I fully accept that ultimately the will of the people expressed through their elections has to drive what we do. So you need to be close to the political sense in that sense, but not so close that you simply make all the mistakes that overpoliticized leaders of very difficult national security enterprises can make.

Chairman LIEBERMAN. Right. That was a good statement. You have to be mindful of the political realities that the President is facing, but also obviously tell the President the truth, as you see it.

One of those little questions that always comes up: How important to the DNI's strength and credibility is it that the DNI himself be there at the daily intelligence briefing for the President?

Admiral BLAIR. The approach I took—and it felt right for me and this President—was that I was responsible that the intelligence—the daily briefing of the President was correct, but I did not have to be the one to brief it every day. So I think it is the former responsibility that is the more important. And then I think that the President—a DNI needs to attend enough of those sessions so that he gets a sense from the President and his inner circle as to are the right questions being answered and so on, and he needs to do that, I think, on a fairly frequent basis. I would always receive a memo from the person who gave the briefing, here is what happened, here is what the President asked and so on. I mean, that is natural. But it is not quite the same as being there and seeing, we are just not hitting the mark on this one so we need to work on it better.

So I think you need to be there for some of the time but not wear out your welcome.

Chairman LIEBERMAN. Last week, incidentally, at the hearing everybody agreed, including those who had had most of their experience at the CIA, that the DCI was an unsustainable position, it was too much, and that, therefore, creating the DNI made sense.

I want to say in passing that General Michael Hayden said something interesting, which was that he thought that he was probably the only Director of the CIA who was nominated since we have had a DNI who was actually recommended by the DNI, and he thought that was not good. He was recommended because he knew Admiral Mike McConnell or Admiral McConnell chose him, but that the others had come up, as would naturally happen, through the White House. I do not know—unless you want to comment, but I was really saying that more to share it with you as an interesting historical observation.

Admiral BLAIR. I just have one comment on that, if I could, Senator Lieberman.

Chairman LIEBERMAN. Go ahead.

Admiral BLAIR. I strongly believe that the Director of the CIA, whether it be the CIA as we now know it or the CIA as I recommended it, with an analytical piece and a clandestine piece, should be a CIA professional that has come up through the ranks. I think the record shows that those who have done that have been some of the Directors of the Central Intelligence Agency that we think the most highly of their records.

I think now that we have a DNI position, that is the position that you should put someone who should have some intelligence knowledge but does not necessarily have to have lived and breathed it all his or her life. But I think part of the confusion in roles that we now have is when you appoint two people to these two jobs, both of whom are sort of considered independently rather than one being a professional. We get some of the jostling that we have seen in recent times, and I think the political direction can be sent through the DNI, and we ought to have professional DCIAs.

Chairman LIEBERMAN. I think that is a big insight, and what it requires is a President having different visions of both roles and really recognizing that the DNI is the President's main personal intelligence adviser, and also in the President's interest, the leader of the community.

General Hayden did not dwell on it, but when he made his statement, he included the incoming head of the CIA because there is no one in the world who thinks that General Clapper came up with the recommendation of General David Petraeus to head the agency—not that he is opposed to it, but your point is well taken.

I want to ask you just to dig down a little bit deeper on it, and then I want to ask you about the split in the Agency that you recommend.

Talk a little more about what the advantages are of having a career person at the head of either the CIA as it is now or a CIA in two parts.

Admiral BLAIR. I think the main advantage, Mr. Chairman, is that you have someone who knows the organization. If you choose the right person, as you should, that person will have instant credibility and a following. I think with agencies whose jobs are special-

ized and difficult, you just cannot walk in and do them with a general purpose background, that the best leaders move their organizations a step further, to be more skilled, more unified, and able to do new things. And I think that is really best done by somebody who knows the organization.

I am also influenced by what I saw at the CIA in that there are marvelous people there. I saw any one of four people in that Agency who I, had I had the chance, would have recommended to be the Director. You had four good chances, and you could have flipped a coin among them. So there are good people there who can do it. And if you have a DNI who is running the political top cover for them, then you can have your Director of the CIA being a professional just the way a uniformed military officer or a police chief is.

Chairman LIEBERMAN. Sure.

Admiral BLAIR. I mean, that is what they do. And so I would say that is part of it.

And, finally, as I said, as I looked back over the history of Directors of Central Intelligence, although there has been some brilliant work done by outside officers coming in, if you had to handicap the odds, those who were remembered as having done the best at a higher percentage rate are those who have the background. So that is really what I think the advantages are.

Chairman LIEBERMAN. Now go in a little bit deeper than you did in your opening statement about why separate the CIA into an analytic section or agency and a clandestine agency.

Admiral BLAIR. Yes, Senator. Starting off with trying to clean the slate and letting us look at those two different functions, they are really quite different approaches. An analyst is skeptical, questioning, uses the academic skills and all. A case officer or an officer involved in covert operations has got to be positive, extemporaneous, flexible doing the job. So you have oil and water here in terms of the sort of people who do it.

Until I guess about the early 1990s, of course, they were originally divided out at Langley. This tower was the analyst tower and this tower was the operators' tower. When they were thrown together and mixed up, there were some advantages. I think the main advantages were for the clandestine service, the operators, because it gave them a closer sense of what was required, and they could direct their efforts more to that. It taught them to become a little more reflective in what they were doing, not just where is the job, let us go do it, where is the door, I want to run through it. So there were certain advantages to that. And I would leave an analytical cadre in the national clandestine service in order to perform that function.

But also over time the operator ethic prevailed at the Agency. Being the sort of active can-do people they are, they were the ones who pretty much set the tone for the Agency. And I think it, detracted somewhat from the analytical ability and made it difficult analytically at some times, especially when the analysis was not supporting the program that the action side was working on.

In addition, if you look at where the intelligence comes from now—I do not have the figures right with me. They may well be classified. But the bulk of information comes from signals intelligence gathered by the NSA. So it is not that you have the all-

source analyst next to the place where most of the intelligence is coming from. So I do not see any disadvantage to having this all-source analytical shop separate and then the clandestine service would be the specialists in human intelligence. They would feed it in. Signals intelligence comes in. Geospatial-intelligence comes in.

In the same way, as you will recall, when the National Geospatial-Intelligence Agency was formed, intelligence analysts were taken out of the CIA, put together with the same skills from the Defense Mapping Service, and they were the functional experts on geospatial intelligence, and they now help the CIA just the way they help others. So it is sort of an analogous thing of having the functional division of the collectors fairly pure and the analysts together.

Now, the danger in that thing is that people get back in their stovepipes and they do not cooperate, and that is where I think the DNI putting these mission management teams together with representation from all of these agencies is the norm.

Just a final point. I think you will find that the United States is completely unusual in having this particular collection of skills. If you look in other countries—and it is not that we should be bound by other countries, but it is just sort of an interesting check of how it happened. It is more a product of our history than it is a product of how it is generally done around the world.

Chairman LIEBERMAN. I had not thought about this. There is a separation between the operators and the analysts in most of the foreign intelligence.

Admiral BLAIR. Correct. In most foreign intelligence, they are separate.

Chairman LIEBERMAN. I must say that I had followed these things from a distance, but when I came here as a Senator and started understanding what the CIA was about, I was surprised at how many people I would interact with in briefings who I would call basically researchers. It was valuable research. They were becoming expert in a particular country. But most—not all, but a lot of what they were doing was from open sources, and that is necessary. That is actually very important, but not what I think the public feels is the CIA. The public thinks of it as the operators and the clandestine workers. Those are two very interesting suggestions.

Let me talk to you about another one that I think is interesting, and it does relate to the Osama bin Laden case, which is, as you indicated briefly in your opening statement, we have Title 10, which covers traditional military operations authorized by the President; then you have Title 50 covering intelligence and covert authorities. As you and I have discussed and is known, in the case of the Osama bin Laden search, the President gave the authority to the Director of the CIA, which was interesting, under Title 50—and Director Leon Panetta has been very open and enthusiastic about this. He called on the Joint Special Operations Command, Admiral William McRaven, operating under Title 10. So you make a very interesting and I think relevant suggestion here that we effectively need, as you said, a Title 60 for what you called joint integrated teskforces.

So let me ask you to develop that a bit. I presume it comes from the fact that, as you said during these questions and answers, a lot of what intelligence operators are doing today is inherently joint, but these actions particularly are. So what would be the benefit of a Title 60?

Admiral BLAIR. Sir, let me illustrate it first by a well-known bad example since I think that is always instructive.

Chairman LIEBERMAN. Yes.

Admiral BLAIR. If you recall, when we went into Afghanistan late in 2001 and CIA agents famously rode in rickety old Russian airplanes with bags of money between their legs, and when they got out, they started reaching their old contacts, paying them money, turning the Northern Alliance. Meanwhile, Secretary Rumsfeld was famously impatient that the special forces were not there yet. They were slow, they were getting in place ready to jump, and never again will DOD be second getting into one of these situations. There was explicit competition between those two groups to get in and do the same job. And then, tragically, when a number of CIA agents were killed with a group of Afghans who had been taken prisoner and the CIA officials were outnumbered and beaten to death, the military back-up for that was not readily available. And yet it is one country, one President, one Congress, one set of authorities.

What we need to do is put the best capabilities of the Defense Department that applied to this problem together with the capabilities that the CIA can bring, integrating a staff so that you have knowledgeable direction, and then using everything, whether you are utilizing all of the skills that the CIA has developed in terms of working with foreign intelligence services—the CIA has a lot more budget flexibility than DOD does. In those situations I think it is very useful. But yet having the huge back-up logistics, planning capability, and fire power that the Department of Defense can bring to bear is also important.

What I want for the country is let us do them both. Let us not have the President have to make a decision. Do I give this one to the CIA or do I give this one to the Department of Defense?

Now, the other thing that has happened is that the definition of covert action under Title 50 has really changed since the Cold War when it was invented. It was basically to make actions deniable so that we could take lethal action against the Soviet Union and areas around the world. We could officially deny it. We would not risk escalation to World War III. If there was ever an operation which was less intended to be deniable than the raid 2 weeks ago on Osama bin Laden, I have no idea what it was. That does not pass, I do not think, anybody's traditional understanding of what a covert action is. We were going to do it. There were going to be soldiers involved. There were going to be sailors involved. The CIA was going to be involved. Five thousand people were probably involved in that operation from the very beginning, and we were going to do it. Why? Because it was a job that was not being done by a country that we could call on to do it, and we felt we had to do it ourselves.

That is really the nature, I think, of the challenge we face now with al-Qaeda and its affiliates, drug cartels, outlaw operations of

various kinds, even some outlaw countries. It is not the state boundaries Cold War that we invented plausible deniability to take care of.

In addition, a lot of these campaigns go on for a long time, like our current campaign in Afghanistan, and, again, if there is a more publicized CIA action than drones in Pakistan, I do not know what that is. The CIA officers call reporters and tell them about what happened on a routine basis. So I think these definitions are getting in our way, not helping us.

What they do set up is sort of a competition for who is in charge rather than a mechanism so that both sides can bring it to bear. So I am for doing it.

Now, there are some very weighty questions involved. Title 10 is part of what entitles soldiers to protection under the Geneva Convention and under Status of Forces Agreements. So Title 60 would have to be designed in a way that, yes, this is still a military action, these are still soldiers, if they are captured, so on and so on.

Now, again, that provides some protection, but had one of the helicopters gone down in North Waziristan and the Haqqani tribe picked up some of our SEAL Team 6 people there, I doubt if they would have been much motivated by the Geneva Convention, and that is generally how it is in these situations.

Similarly, who does this group report to and to whom is it accountable in Congress?

Chairman LIEBERMAN. Yes, I was thinking about that. In Title 50, there is a requirement for quite limited notification to Congress of covert action. Obviously, under Title 10, special operators are operating all the time with no notification for Congress. So how would you balance that?

Admiral BLAIR. Within Title 60 I would say that both Intelligence Committees and Armed Services Committees need to be notified. There was one instance of a somewhat similar operation that I was involved in when I was in DNI, and we formed a joint briefing team. We went up and we talked to the leadership, both Houses, both parties, about a very sensitive operation that involved military and intelligence community actions. And, the world did not come to an end. They asked good, tough questions. We were able to answer them. I think we can do the notification part of it well.

So I think we need ways to draw those capabilities together for the country.

Chairman LIEBERMAN. Who would be in charge of one of the joint task forces?

Admiral BLAIR. I would look at it and say that you know this is a mixed set of skills here. On balance, is it 51 percent intelligence and 49 percent military, or is it the other way around? And I would choose the lead commander on that basis. But the deputy I would make from the other discipline so that you have the two top people bring both sets of skills to bear. And also I would make sure that those two top people had qualifications and experience with operating with the other agencies, similar to the way we do it with joint commanders.

Chairman LIEBERMAN. Right.

Admiral BLAIR. But I would mix them, and I would have the staff mixed so that you had all the skills available to spark that synergy and to keep from doing something stupid in either the intelligence or the military realm.

Chairman LIEBERMAN. Would the DNI be always involved in one of these joint task forces?

Admiral BLAIR. I would say that his involvement would be comparable to that of the Secretary of Defense: Final approval for the plan, approval of the commander, and concurrence with the deputy. And then if you are a good DNI, just like if you are a good Secretary of Defense, if you have chosen good people, given them good direction, approved a good plan, you let them roll.

I hand it to the current leadership for what I understood of what happened during those hours of the raid. They sat there and let the people who were right there make the decisions, and that is the way it ought to run.

Chairman LIEBERMAN. Yes. Those are very interesting ideas. I think I have, within the rules of the Geneva Convention, interrogated you enough today. Admiral, you have been extremely helpful, and Senator Collins and I talked about it briefly on the floor. You have given us some ideas. I am not quite sure what we are going to do from here. We may recommend some additional legislation if it makes sense; I think some of these really do require it. In other cases, we may issue a report and make recommendations to the President or to the DNI. But if you are willing, I reserve the right to reach out and just call you on the phone or ask you to come in and talk about the direction in which we are going, because the combination of your experiences in service of the country is really quite unique and very helpful. Also, you have had the independence now out of office to make some of the suggestions that people in office sometimes do not make. So this is what I have to look forward to after January 2013.

Admiral BLAIR. I hope we can call on your wisdom after you leave that chair, too, Senator Lieberman.

Chairman LIEBERMAN. Thank you. You always can do it, whatever wisdom there is there. I thank you. I thank your wife for being here with you. I even thank my friend for decades, Arthur House, and your friend and counselor, for being here.

We will keep the record of the hearing open for 15 days for any additional questions or statements, but, again, with great thanks to you for what you have contributed today.

The hearing is adjourned.

[Whereupon, at 3:18 p.m., the Committee was adjourned.]

SEE SOMETHING, SAY SOMETHING, DO SOMETHING: NEXT STEPS FOR SECURING RAIL AND TRANSIT

WEDNESDAY, JUNE 22, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:33 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Carper, Landrieu, Collins, and Paul.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. Thanks very much to our witnesses for being here, and thanks for coming a bit earlier than we had planned to start the hearing. Senator Collins and I may be called to the Senate floor at 11 a.m. when a bill from our Committee is pending.

Mr. Pistole, you will be happy to hear that this is a bill to reform the process by which nominations are made and considered by the Senate.

Today, we have come together to discuss the security of our rail and transit systems and strategies for the future to improve the defense of these systems, which are historically open and, therefore, in the post-9/11 world, vulnerable.

This hearing is being held as part of a continuing series of hearings and investigations our Committee has committed to do as we approach the 10th commemoration of the attacks against America on 9/11. But in this particular case, this hearing was also catalyzed by the reports from the raid on Osama bin Laden's compound in Abbottabad, Pakistan, which yielded documents indicating that Osama bin Laden continued to urge members of al-Qaeda to attack the rail sector of the United States, particularly on or about the 10th anniversary of September 11, 2001. Apparently, one of those documents included a plan to derail a train. Some of the analysts that we have talked to have concluded that the most likely form of such an attack would be multiple operatives acting independently against separate targets as part of a coordinated attack on the same system and, of course, usually at peak travel times. There has also been some reference to Osama bin Laden suggesting that

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00099 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

these kinds of attacks might most dramatically occur on rail lines over valleys or bridges.

In other words, this again made real the threat to our rail and transit systems, which we have lived with since 9/11 and, of course, we have seen carried out in other places like Mumbai—the first attack—Madrid, London, Moscow, and, of course, plans which were thwarted to attack rail systems right here in Washington, DC, and in New York City.

In fact, the Mineta Transportation Institute [1] issued a report that concluded that since September 11, 2001, worldwide—this is a stunning number—1,800 attacks have been carried out on surface transportation, mostly buses and trains, obviously not all of them major, causing over 3,900 deaths. Compare that to the 75 attacks carried out on airplanes and at airports that have caused about 160 deaths—157 to be exact.

The other fact here is that 14 million people use mass transit systems in America every day. In Connecticut, the Metro-North New Haven Line is one of the busiest rail lines in our country. Speed, reliability, and convenience are obviously hallmarks of mass transit, and we support mass transit as part of broader societal goals. But with so many passengers at so many stations along so many paths, those systems are very difficult to secure.

We certainly have not gone unsecured, and since 9/11, we have increased the presence of surveillance cameras, explosives-detecting dogs, roving security teams, and, of course, a greater public awareness. Secretary Janet Napolitano has energetically promoted—and Mr. Pistole also—the "See Something, Say Something" public education campaign because the security of our rail system really does hinge in large part on the awareness and actions of an observant citizenry.

But a decade after 9/11, as one of our witnesses, Dr. Steve Flynn, correctly suggests, we need to move beyond "See Something, Say Something," to "Do Something."

Rail and transit security has been traditionally the primary responsibility of State and local law enforcement. However, the Transportation Security Administration has begun to play a critically important role. TSA has been working with State and local governments to improve rail and transit security. It now has 25 mobile security teams, known as Visible Intermodal Prevention and Response teams—one of the best acronyms that I think our government has—that it sends into the field. The President's fiscal year 2012 budget requests 12 more such teams.

TSA also has over 300 security inspectors working with local transit officials to assess the security of trains, platforms, and rail yards. But there is more that TSA, State and local governments, and transit agencies can and, I think, must do. Let me just mention a few.

First, TSA really needs to fulfill a 2007 legislative requirement to develop uniform standards for rail and transit training programs for background checks for front-line employees and for transit agencies' security plans.

[1] The document referenced by Chairman Lieberman appears in the Appendix on page 462.

Second, the Department of Homeland Security should step up its efforts to develop creative, non-intrusive transit security solutions, especially to detect improvised explosive devices, which history has shown are the weapons of choice for disrupting rail and transit systems. The Department of Homeland Security has a Science and Technology Directorate explicitly to achieve this, but specific R&D for rail and transit security innovations, in my opinion, has been much too limited.

Third, TSA has to improve its intelligence sharing with State and local officials—it has come a long way, but it needs to come further—and also the private sector, to provide information that is both current and useful to them, that is, simplified and easier to manage.

Fourth, all of the stakeholders in transit security need to be conducting more exercises to accustom rail and transit officials with the unique requirements of disaster prevention and response involving mass transit, particularly trains. So I hope that TSA and FEMA will continue to expand these exercises and that local and State authorities will become more proactive and ensure that employees at every level are involved.

And fifth, we have to continue to work with passengers to make them full partners in securing our rail and transit systems, and that includes educating them about the risks, how to report suspicious activities, and how to respond should an attack occur.

We have the Department of Homeland Security's Transit Security Grant Program through which approximately $1.8 billion in rail and transit security grant funds have been distributed since 2006. These funds are critically important to our State and local authorities, and that is why I feel that the House action to zero out these funds is just plain bad policy, and I hope we will be able to overturn that legislation here in the Senate.

I do want to stress that our law enforcement and intelligence agencies have successfully thwarted plots against rail and transit systems, and we should not, in talking about what more we can do, pass over that without acknowledging really remarkable work. The 2009 plot by Najibullah Zazi to explode bombs in the New York subway system was disrupted by brilliant intelligence and law enforcement work. A threat to the D.C. Metro system just last year was similarly uncovered and stopped before anyone was hurt.

So these are some of the subjects I want to take up with our witnesses. We really have the best in the field before us in the three witnesses, and I thank them for their commitment to strengthening the security of our rails and mass transit and for being with us today.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

First of all, it is a pleasure to welcome back to our Committee Administrator Pistole. It has been about a year since his confirmation, and I very much appreciate his commitment to strengthening the safety and security of our transportation infrastructure and our travelers.

I am also pleased to welcome Commissioner Boynton here from Connecticut to lend his perspective from the State level and, of course, Stephen Flynn, who has testified before this Committee many times and provided us with his insights.

As the Chairman has pointed out, today's hearing on rail and transit security is timely. Only a few days after our U.S. Navy SEALs raided Osama bin Laden's compound, the Department of Homeland Security and the FBI released an alert about rail security. The information was dated from early last year and was not connected to any particular city or rail line. Nevertheless, it demonstrated and reminded us that mass transit remains a terrorist target.

The fact is, soon after 9/11, terrorists began targeting mass transit systems. In March 2004, 10 bombs exploded on four commuter trains heading into central Madrid. The attacks left 191 people dead and 1,800 people wounded in what is regarded as the worst Islamist terrorist attack in European history.

The United States has been subject to rail plots as well. Since 2004, our government has thwarted five terrorist plots against our Nation's transit and rail systems. Metro and subway stations in New York City, here in Washington, DC, and train tunnels between New York and New Jersey were the intended targets.

While improvements have been made since 9/11, the challenge of securing rail and mass transit systems is enormous. As the Congressional Research Service reported in February, passenger rail systems, particularly subways, carry about five times as many passengers each day as the airlines over many thousands of miles of track, serving hundreds of stations that are designed for easy access by passengers. The vast network and sheer volume of riders make it impractical to conduct airline-type screening. Security at airports is the responsibility of the Federal Government, but security at subway, bus, and rail stations is largely under the jurisdiction of mass transit providers in partnership with State and local governments.

It is vitally important, however, that the Federal Government act in concert with these local partners, helping to ensure that transit providers and local officials have the equipment and the training to plan for and to respond to terrorist threats while ensuring that taxpayer dollars are spent efficiently. I would note that the same CRS study says that much of the training is directed at response rather than prevention.

In addition, Federal agencies must partner with State and local law enforcement to develop a process to identify and report suspicious activity and share that information nationally so that it can be analyzed to identify broader trends.

The GAO recently reported that transit administrators and public transportation professionals currently receive security information from a variety of sources. Nearly 80 percent of the respondents used five mechanisms or more to receive security information. The GAO identified at least 21 mechanisms through which agencies can receive security-related information. The GAO noted that those interviews yielded a common desire that the information should be streamlined to reduce the volume of overlapping information that public transit agencies receive.

As we work to improve and streamline information sharing, we need to remember that an alert citizenry remains our first line of defense against terrorist attacks, whether at transportation hubs or city parks or airports or in Times Square. A good example is how an alert street vendor, noticing smoke coming from a vehicle in Times Square, reported it to local law enforcement and thus helped to disrupt an attempted bombing. If not for this concerned citizen, the consequences could have been deadly.

In 2007, Senator Lieberman and I co-authored a law that made it easier for alert citizens to report suspicious activity in the transportation sector indicating potential terrorist behavior without facing the threat of frivolous lawsuits. This year, we have reintroduced our See Something, Say Something bill to expand those protections to reports of such behavior in all sectors.

The world is a safer place without Osama bin Laden, but we are not yet safe. We are better prepared for terrorist attacks across all modes of transportation, but the fact remains that future attacks, at least attempted attacks, are certain. The enemy continues to innovate and probe our defenses.

Administrator Pistole and I recently spoke at a forum conducted by the U.S. Chamber of Commerce about these challenges. One of our greatest assets is the spirit of innovation and flexibility that is fostered when we partner with the private sector, State and local governments, and local law enforcement officials. We are able to benefit from their eyes, ears, and ideas.

I thank our witnesses for being here, and I look forward to the discussion today.

Chairman LIEBERMAN. Thanks very much, Senator Collins.

I thank Senator Paul and Senator Carper for being here. We will go now to Administrator Pistole. John Pistole has spent 28 years in the service of our government. We talk a lot about service in the military, but people like Administrator Pistole have served our country with great effect—we appreciate it—most of that with the FBI and now with the TSA. So we look forward to your testimony.

TESTIMONY OF HON. JOHN S. PISTOLE,[1] ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PISTOLE. Well, thank you, Chairman Lieberman, and Senators Collins, Carper, and Paul. I appreciate the opportunity to appear before you today with the distinguished co-witnesses to discuss the efforts of TSA in partnership with not only DHS and FEMA, of course, but our industry partners and those who are in the best position to provide the best possible mass transit and passenger rail security.

Chairman Lieberman, I would just comment on your five goals for improvement that you noted in your opening statement, and I agree with each one of those, noting that we have made some significant improvement in those areas, but we need to do more. And so I appreciate your highlighting those.

As has been mentioned, last month the President announced the U.S. operation that resulted in Osama bin Laden's death, and that

[1] The prepared statement of Mr. Pistole appears in the Appendix on page 442.

effort marked a historic counterterrorism success for not only the United States, but for the world. And I would add to that the recently announced deaths of Ilyas Kashmiri, the leader of an al-Qaeda operational wing out of Pakistan for Western attacks, including Europe and the United States, and Harun Fazul, the leader of al-Qaeda in East Africa and, of course, the leader of the 1998 East Africa bombings and much of al-Qaeda's work in the Horn of Africa there.

Our efforts to combat terrorism go well beyond those individuals, as Senator Collins mentioned, and that is why we remain focused on trying to do what we can do in terms of enhancing the efforts of others along with our own critical mission of protecting the traveling public and our transportation systems.

TSA will continue to evaluate screening measures based on the latest intelligence, and we will continue to share information with stakeholders to enable them to enhance protective measures and surge resources as appropriate.

As we know, mass transit systems and passenger railroads are a critical part of the transportation network TSA works to protect as passengers rely on them for over 10 billion trips annually. They also remain a target for terrorist groups and have been the subject of numerous attempted plots in the United States, two of which were mentioned earlier, as well as a number of successful attacks overseas, which have also been noted.

Passengers serve as important partners for securing these systems, and we are encouraging Americans to alert local law enforcement if they see something that is potentially dangerous through the nationwide expansion of the "If you see something, say something" campaign, a clear and effective means to raise public awareness of indicators of terrorism, but also crime and other threats, and emphasize the importance of reporting suspicious activity to the proper law enforcement authorities.

Our partnerships with industry and local and regional stakeholders are a critical component of TSA's security efforts for mass transit and passenger rail. DHS's comprehensive Transit Security Grant Program is currently the primary vehicle for providing funding assistance for security enhancements to eligible transit agencies, supporting State and local government initiatives to improve security. TSA works with FEMA to fund projects that most effectively mitigate risk at the highest risk systems. In other words, how do we best buy down risk?

These projects address operational deterrence activities, the remediation of critical infrastructure in transit, and other assets critical to surface transportation security. In 2010, DHS awarded nearly $274 million to the transit and passenger rail industry, bringing the total to over $1.6 billion awarded since 2006.

In addition to grant funding, TSA supports the security of mass transit and passenger rail systems by deploying those VIPR teams that Chairman Lieberman mentioned to augment the local security efforts. We do have 25 dedicated teams in operation, and we are seeking to expand that to an additional 12 teams in our request for the 2012 budget.

Now, the VIPR teams work alongside local law enforcement officers and are typically comprised of personnel with expertise in in-

spection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to deter potential terrorist attacks.

VIPR teams enhance TSA's ability to surge resources quickly anywhere in the country. TSA conducted over 8,000 VIPR operations in the past 12 months, including over 4,200 operations in mass transit venues across the country. In addition, TSA performs baseline and collaborative risk assessments for mass transit and passenger rail, engaging State and local partners in three critical areas: One, how to reduce vulnerabilities; two, assess risk; and, three, improve security efforts.

These assessments are conducted with emphasis on the 100 largest mass transit and passenger rail systems in terms of passenger volume, which collectively account for over 80 percent of the more than 35 million trips taken on mass transit each weekday. Among these assessments is the Baseline Assessment for Security Enhancement, a comprehensive security assessment program designed to evaluate 17 security and emergency management action items that form the foundation of an effective security program. Through the BASE program, TSA reviews security-related proposals jointly developed by TSA, the Department of Transportation's Federal Transit Administration, and private sector partners from mass transit and passenger rail systems. The assessment results provide critical data about security priorities, the development of security enhancement programs, and the allocation of resources—a critical aspect, obviously—and a compilation of the most effective security practices for mass transit and passenger rail agencies. Over 115 mass transit and passenger rail agencies have participated in the BASE program and used their assessments to help make their systems even safer and more secure for their passengers, employees, and infrastructure.

TSA also provides timely, relevant intelligence and security information to industry officials and State and local partners, and we are working with our partners to develop a unified, comprehensive intelligence and security information-sharing platform for that mode.

In closing, I would like to stress again that collaboration is critical for the success of mass transit and passenger rail security operations, noting that no one single agency can do it all. TSA will continue to collaborate with law enforcement, industry, State, local, and tribal officials, first responders, and Federal partners to foster regional security coordination and enhanced deterrence for response capabilities.

With that, Chairman Lieberman and Senator Collins, I would pause for questions and other statements. Thank you.

Chairman LIEBERMAN. Thanks very much for that opening statement.

We will next go to Peter Boynton, Commissioner of the relatively new Connecticut Department of Emergency Management and Homeland Security. I am really delighted that you could be here today. We look forward to hearing from you about the State and local perspective on securing mass transit, particularly in our State, which, as I said in my opening statement, has such heavy

rail traffic. Thanks for being here, Commissioner, and we welcome your statement now.

TESTIMONY OF HON. PETER J. BOYNTON,[1] COMMISSIONER, CONNECTICUT DEPARTMENT OF EMERGENCY MANAGEMENT AND HOMELAND SECURITY

Mr. BOYNTON. Thank you, Chairman Lieberman, Senator Collins, and Senator Paul. I appreciate the invitation to come here today. I am here to offer a State perspective, as you said, Mr. Chairman, and I also come with some other background. I was the TSA Federal Security Director for a couple years at Bradley International Airport in Connecticut, the second largest airport in New England, and I was also the Coast Guard Captain of the Port in New Haven, Connecticut. So I hope that does not mean that I cannot hold a job.

Chairman LIEBERMAN. No. It really reveals to everyone that there is a heavy Coast Guard tilt on this panel.

Mr. BOYNTON. Yes, sir. I am afraid you have broken our cover. [Laughter.]

I would like to begin by thanking the terrific partnership that we have in the State of Connecticut, and it is an example of what I think you and Senator Collins already indicated is a lot of work already done and achieved. And this includes MTA and Amtrak police who work with us in Connecticut, TSA in Connecticut, the Coast Guard, Connecticut State Police, Connecticut DOT, all the first responders who are there on that rail line every single day. DHS has done a terrific amount of work to support the Connecticut Intelligence Center, a State-run entity that we really rely on DHS to support, and, of course, all the public who participate in our See Something, Say Something campaign that we rolled out last summer.

Connecticut does have a mass transit rail system, but it also has a number of other mass transit forms. We have two ferries that go to Long Island. They are two of the 14 largest passenger/auto ferries in the country. They are the only two that are privately operated. We have a number of bus systems throughout the State. We have a number of rail systems—the Northeast Rail Corridor, a rail corridor from New Haven up through Springfield. But the one I would like to focus on is the Metro-North New Haven Line.

This system carries 127,000 passengers every day, 289 trains every day, and even so, it is not among the largest. But what I think is very notable about that the Metro-North New Haven Line is its connection with New York City. It is part of the much larger New York City metropolitan system. And every one of those Connecticut riders go right to the heart of New York City—Grand Central Station from New Haven and other points on the line. In 2010, there were over 37 million passenger trips from Connecticut into New York City.

My point here is that the interconnected nature of mass transit means that the security of the New York City system is dependent in part on the security of the Connecticut-based part of the transit system, and that is not unique to Connecticut. We see that with

[1] The prepared statement of Mr. Boynton appears in the Appendix on page 450.

communities that surround urban areas with transit links all around the country.

From the State perspective, however, what we are seeing is Federal funding increasingly being shifted into the large urban areas. This is not only happening with transit security, but also with UASI grants and shifts in port security. The focus on security for cities makes sense for a lot of reasons, but shrinking funding for those surrounding communities with transit links into those urban areas may have the unintended consequence of pushing the risk out to those surrounding areas. And Connecticut has real experience with this. The 9/11 terrorists and the attempted bomber in Times Square both spent time in Connecticut.

So our view is that the challenge is to modify some of the current Federal Transit Security Grant Program criteria to include more proportionate funding for those communities outside of the major urban areas but with transit links into those major urban areas. We may be a relatively small transit system, but because we are part of the larger one, their security depends on our security.

We need additional funding to continue to complete some of the basic security enhancements that have already begun, and these are basic things: Fencing, lighting, communications, cameras. A specific example is that under the new criteria for the Transit Security Grant Program, Connecticut is unlikely to continue to receive transit security grant funding this year except in Category 1 for public awareness, which is very important. We need more of that money, and we will use that money well. But we are unlikely to qualify under the new criteria to complete some of those enhancements that we have already done. And, again, it makes sense to focus on the urban areas, but we are part of the urban areas, and there is a potential vulnerability by pushing that risk out to us.

In addition to modifying the grant criteria, there may be some utility to using the model used in the Port Security Grant Program whereby the local Coast Guard Captain of the Port convenes a group of users to help evaluate and prioritize the grant submissions. Potentially, the analogous person to do that might be the TSA Federal Security Director, pulling together users of the transit system to help us do an evaluation of those grant proposals. We have produced something like that in Connecticut that I will talk about a little bit later.

I would also like to note that, at least from our perspective, balancing the grant criteria for some proportional funding for the surrounding communities—and we are really talking about small dollars—is linked to the evolving terrorist threat. On the one hand, the Federal partners have helped us understand how this threat is evolving. The diversification of the threat is essentially requiring more involvement from the local community level. But, on the other hand—and this would be the Federal hand with the money—it seems in some respects to be going in a different direction, and that is, increasingly focusing funds within the city limits of large urban areas. And those of us who are connected with mass transit really have a need not just for our own State and our own population, but as a partner with that urban area to help them stay safe as well.

In addition to balancing the grant funding to achieve transit security, another way is to enhance information sharing, and this was the point I mentioned earlier. In Connecticut, we have convened a Transit Security Committee. We have representatives from every mode of transportation: Rail, bus, trucking, highway, aviation, maritime, even pipelines, all working together.

We have all heard of the danger of people operating in silos. One of our local partners just a couple weeks ago gave me a new term to use, and the term was "cylinder of expertise." We all have cylinders of expertise, and those are not bad things, but the difficulty is pulling them together with horizontal integration, and this pulling people together does not happen without effort. We have to take people out of their comfort zones and get them to work together, and we have had great success through that committee.

Another example of pulling people together from within their cylinders of expertise are the VIPR operations that Administrator Pistole mentioned. In Connecticut, I just have to give thanks to our TSA partners. In 2009, we had 34 VIPRs. By the end of this year, we expect to have increased that seven-fold. These VIPRs do not happen without the leadership of a TSA Federal Security Director coming out of the comfort zone and working with other Federal, State, and local partners to make it happen, and it is a big success in Connecticut. I would like to see more support on that.

Another example of pulling people out of their silos of expertise or cylinders of expertise is the intelligence fusion center. In addition to the traditional partners—State police, DHS, FBI—we also have a full-time TSA intelligence analyst, and I do not know how many of the 72 fusion centers have a full-time TSA analyst. We do in Connecticut. I hope by mentioning that I have not put that in jeopardy because we want that person to stay. That is his primary work location, and it gives us tremendous information exchange, not just with the State. We have full-time municipal police detectives whose primary job location is in our fusion center. That allows us to marry them with the great work of TSA pulling information into our fusion center.

Last, and probably most importantly, is engaging the public. We have a very substantial See Something, Say Something campaign that has been running for 2 years in many different media routes. But I certainly agree the next step is to go beyond seeing and saying to doing something. And I think we have a great example in the area of emergency medical response, and that is, publicly available defibrillators. If we talked 30 years ago about allowing members of the public to operate a defibrillator, I think we would react in horror. But today we do that. We have come that distance. And I think we can do the same in the area of security by engaging the public not only to see and say but also to do, and that is a great principle of resiliency. It is an example of adapting if we can get to that next step of helping people do something.

Thank you very much for the opportunity to be here, and I look forward to answering questions.

Chairman LIEBERMAN. Thank you very much, Commissioner Boynton. That was very helpful.

Finally, we will go to Steve Flynn, a former Coast Guard Commander and now President of the Center for National Policy. He

has been a really terrific resource for this Committee over the years, and we welcome you back with gratitude for your testimony today.

TESTIMONY OF STEPHEN E. FLYNN, PH.D.,[1] PRESIDENT, CENTER FOR NATIONAL POLICY

Mr. FLYNN. Thank you so much, Mr. Chairman, Senator Collins, Senator Landrieu, and Senator Paul. It is an honor to be here today. What I would like to do is to offer a bit of an analytical perspective about the threat, why I think this hearing is so important, and then speak to a few don'ts I would suggest about how we approach this issue, and then some ideas about the do's, where we go from here.

I would offer up at the outset that we really are still at the starting line, and as with so much in Washington, we can always evaluate priority by what we spend, and the numbers are pretty clear on this one. We spend on average $9 for every passenger who flies, and the estimate for the amount of money that we spend on transit is a penny or a little less. So that kind of tells us where we are in terms of what we have been willing to invest in.

Now, this is not to say that we should replicate the model that we are doing in aviation and do a very expensive effort with regard to transit. The heart of my testimony here today is to say, in fact, this is an opportunity, since we are still at the starting line, to essentially recalibrate the approach.

I want to specifically speak to the threat and why I think that we really need to step up our focus on this area, and it is not simply because, as was laid out at the very outset of your opening statement, Mr. Chairman, we know Osama bin Laden had been plotting and thinking about the transit system. We have the very explicit examples from around the world of attacks since 9/11 on those systems. But the threat is evolving. I think there is a convergence of views on this and something that I have been part of being able to track as a result of my being a member of the National Security Preparedness Group led by former 9/11 Commission Chairmen Tom Kean and Lee Hamilton.

Essentially what we are seeing is a fundamental evolution in the terrorist threat with increasingly a homegrown quality, but also with a focus on smaller-scale attacks. And this is driven in part because the capacity to take on large-scale attacks has clearly been hampered. But this has also been because there has been a bit of an "a-ha" moment for al-Qaeda and its affiliates, which is, they realize you really do not need big, spectacular attacks to get big results. You can get a big bang, particularly in terms of disruption, by doing relatively small-scale things that basically lead to a reaction or in many cases an overreaction that is very costly and very disruptive for the society you are targeting.

And so with that we end up with what Commissioner Ray Kelly of the NYPD has called a "let a thousands flowers bloom" kind of strategy where the recruitment threshold is much lower and you are willing to essentially allow lone wolves or an individual with a few allies to go off and cause mischief.

[1] The prepared statement of Mr. Flynn appears in the Appendix on page 454.

Now, that is the broad backdrop against which to evaluate the state of transit security. We have both the homegrown dimension to it and the fact that we are looking at one and two operatives and not looking for necessarily massive, catastrophic scale attacks but things of the ilk that are really disruptive, potentially can achieve mass loss of life, and are very visible sort of attacks. Mass transit and not surprisingly rail freight as well become very attractive to satisfying these two criteria. They are open systems spread across vast geography that are also accessible to the public and that are very time sensitive. Therefore, the ability for a relatively small operation to get into the system is minimal. The goal is to disrupt the system so you do not need massive kinds of things. A derailment or taking out commuters in a single car, if that leads to a shutting down of the system for a period of time or to Washington then coming up on the fly with lots of new requirements to reassure the public, can be very expensive and disruptive.

So what I would suggest is that while we do not have right now immediate intelligence that I am aware of to say that something is unfolding in our cities, we do have enough in terms of general intelligence to say that this is a sector that is being targeted, we have instances of it being targeted in the past, and we need to focus on it to a much greater degree.

So now on to my don'ts. What do we not want to do as we tackle this problem? I essentially would advance here that overall we need to move away from essentially a law enforcement-centric, screening-centric approach to tackling this issue because of both the difficulty of doing so and also because there is an opportunity to take a much different model.

So my first don't is, we should always avoid in any homeland security endeavor, I would argue—and certainly in the case of rail and transit security—alienating the very public that security officials are obligated to protect. This is actually something David Petraeus has figured out in Iraq. Its key is, you need the cooperation and collaboration of the people that you are protecting, and you want to make sure that they see themselves as part of the solution and that they understand the risk and they are playing the collaborative role. We have a tremendous ability within the transportation system to essentially coerce people to comply. You want access to the system, subject yourself to A, B, C. But it is not necessarily the way you win hearts and minds. And given that we have limited resources to be able to bring about something of that scale in the transit system, we should not head down that path.

The second don't is, avoid promising more than you can deliver. This is something that I think is fundamental to governance overall. We do not want to set expectations beyond what we can deliver, and therefore, it is very important to acknowledge there is risk and there are limits to what government can do to eliminate risk when we have an open system that is time sensitive and spread over a wide geographic space—there will be limits to what we can do to prevent acts of terror. And I think the President and the Secretary of Homeland Security should be applauded when they talk about risk as something that cannot be eliminated. This is an important message Americans need to hear.

Now, we also need to avoid the excessive secrecy impulse because if the overwhelming majority of the people we need to talk to, particularly those on the front lines of running trains, are not in the clearance system, then we are keeping them out of the loop. We really need to work much harder, pushing beyond the envelope of the very good things that have been done around information sharing, and encourage Federal players, law enforcement, State and local and security officials to get more information out to citizens, the owners and operators, and the designers of transit systems so that they can start to be a part of the solution set.

So the last piece here is, we need to be very careful not to overreact. When essentially something goes wrong and Americans and elected officials overreact, we are only motivating the very threat that we are trying to prevent.

So the way forward. Essentially, the overarching message I would like to convey—and I was happy to hear it in the testimony provided by both Administrator Pistole and Commissioner Boynton—is that many of these thoughts are clearly in the mix, but we need to put them on steroids. We essentially really need to move away from relying almost exclusively on Federal screening and law enforcement to an effort that basically says for mass transit—particularly, rail, freight, and so forth—we really need to have the public engaged, empowered, and focused on the issue of resilience of the system as a key security imperative.

The reason for this is pretty straightforward. The size and diversity of the system means that we have a lot of passengers and a lot to protect so we need everyone involved. But also I think I want to really highlight the extent to which particularly in transit there is an extraordinary opportunity. If we think about the nature of transit—and I spend a lot of time on the Metro-North Line coming into New York particularly—most transit passengers often end up on the same train at the same time, and many times even in the same seat. They end up knowing the rhythm of that system pretty darn well.

I can tell the story of the Metro-North Line. One of the unofficial rules is, you do not use cell phones before 8:30 in the morning. Somebody who is not aware of this rule and actually starts chatting it up at about 7 a.m. on the train to New York will die of a death glare of 40 other passengers aboard the train. People immediately know the anomaly. In this case, it is not enforceable, but it can feel that you are definitely isolated.

The fact is, folks on that train are aware of their environment. They know the rhythm of the environment. They are vested in that environment. And they are folks that are clearly security assets. It is a little different from aviation. I fly a lot, but it is different airports, different airplanes. I do not have that same feeling for normal and abnormal. Passengers are very much a part of the solution. Of course, conductors, who in many cases know the same faces—they may not know all the names. In some cases they do because some of their passengers are daily commuters. Then there are the people in the stations. We need to expand our security effort to those who own, who operate, and who are vested in the system. These are the passengers and the workers for the transit au-

thorities. How the Federal Government brings them in is absolutely essential to going forward.

So what does that mean? We really need to move the public education effort from "see something, say something so that law enforcement can take care of it" to one that gives them much more granular detail about what they should be looking for, what they should be doing, and how they can help. And what I want to highlight particularly would be the opportunity perhaps to reach out to the major employers who have lots of employees dependent on the transit system and who could convene training that could happen at their workplace to engage those commuters, not as they run for the train, but when they are not in a rush, to sit down and talk a little bit more about transit security. This kind of outreach would certainly be very helpful.

The final thing I want to also mention here is a program in Logan Airport in Boston. It is a program called Logan Watch. Like an airport, the transit system is more than just the trains and the passengers on the trains. We have train stations. We have shoeshine boys and newspaper dealers and so forth, and they should be involved because—again, like we saw with Shahzad—they understand the rhythm of their work environment. Getting them involved is a very important way to go forward.

Logan Watch is a system by which everybody who works in that terminal is given some training—and the goal should be annual training—so that they understand the environment they are in and they can be a help.

I have run out of time, so I just want to conclude by saying that a focus on resilience, which I have been long advancing, is not an exercise in resignation and pessimism. Focusing on our ability to respond and recover to incidents is a way to deter the incident from happening, and so the extent to which we can plus-up more investment in response and recovery, exercises and so forth, for incidents should they happen, both accidental and man-made, the more I think you are going to have a safer system. It does not look like a soft target, going back to what I was saying about the threat. It is, in fact, something that makes sense pragmatically to do, but it also has real value in terms of our goal of hopefully mitigating the risk to the mass transit system.

Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Dr. Flynn. That was very interesting testimony. I am not a regular commuter on the Metro-North Line, but when I do get on the train to go to New York, you are absolutely right that there is a sociology of train travel. There are people there every morning and every afternoon. They know each other. There is a certain extent to which they socialize. There is a certain extent, as you indicated with the cell phone incident, to which they hardly talk to each other at certain hours because they are reading their papers or their memos for the day. Anyway, that was very practical and insightful testimony.

Let us do a 7-minute question round to start. Administrator Pistole, let me begin with you and ask you to focus in, to the extent that you can in open session, on what, if anything, TSA did after the evidence came out of the Osama bin Laden compound in Pakistan that Osama bin Laden was urging al-Qaeda to think specifi-

cally about an attack on a rail system in the United States on or around September 11, 2011.

Mr. PISTOLE. Mr. Chairman, we started off on Monday morning, May 2, following the President's announcement Sunday night, with a conference call to all the key stakeholders and industry as part of a group that is known as the Policy Advisory Group to say that this has happened, just be aware of possible retaliatory action that may be taken either spontaneously by somebody who is a Osama bin Laden or al-Qaeda sympathizer or that may have always been a triggering mechanism if Zawahiri, No. 2 in al-Qaeda, moved up to No. 1. So we did that call just for awareness.

It was then 2½ days later, late Wednesday/Thursday, before the media document exploitation from the compound about that specific threat from February 2010 that noted the rail attack on the 10th anniversary. As soon as we received that information and the declassified portion of that information from the intelligence community, we reconvened that group and then did an intelligence dissemination to all the stakeholders and the industry to say, here is specific information. Now it is over a year old, but it cites an upcoming event, the 10th anniversary of 9/11, and so be aware that, because of the death, that may again trigger some activity to move up from the 10th anniversary.

So there are other things, but those are some of the highlights.

Chairman LIEBERMAN. So is it fair to say that we raised our guard in response to that information from Osama bin Laden?

Mr. PISTOLE. Yes. Actually, in terms of other activity, we also did several things in terms of operational deterrence. For example, the industry on its own, with information from us, obviously, conducted what is known as a Rail Safety Day, and that involved over a thousand law enforcement and security officials from across the country, major transit agencies, that stepped up patrols, either uniform patrols, K–9 patrols, and additional information awareness that given the Osama bin Laden death there may be something going on. So that was done, I believe, on Thursday or Friday of that week, and so that was something that was done based on prior funding from DHS and TSA, but really done unilaterally. So there are other steps that were taken.

Chairman LIEBERMAN. Good. How about the suggestion that there might be an attempt to essentially disable some track over a valley or a bridge? Do we have a way or are transit systems raising their surveillance on tracks to prevent that kind of episode from happening?

Mr. PISTOLE. Yes, and we believe, Mr. Chairman, that this is consistent with Osama bin Laden's idea of trying to cause not only the greatest number of casualties, but as has also been mentioned, the greatest economic impact, plus if you could get a train to derail into a valley, just the psychological aspects of that.

As part of that, the transit agencies, Amtrak in particular, stepped up their patrols of the rails to look at perimeter fencing where appropriate and especially to look at the critical areas over bridges and areas that also may be seen as more vulnerable—obviously to look at CCTV where appropriate, especially at stations. The concern is not only the derailment but also the possible attack like we saw at the Moscow airport where somebody could go into

a crowded station, in this case a train station, whether Union Station, 30th Street Station, Penn Station, with explosives in suitcases or bags, and then do a bombing in that regard. So it is not just limited to the intelligence we have. There has been stepped-up vigilance across the board.

Chairman LIEBERMAN. That is important to hear. The bottom line—and I am saying it to anybody who is listening—is that there is a lot more going on to protect mass transit systems than is visible. It is very visible in aviation transportation, of course, but less so with rail and buses.

Commissioner Boynton, give us the response from a State perspective to the intelligence from the Osama bin Laden compound and, if you can, how you work with TSA, the Metro-North Line, and Amtrak in Connecticut.

Mr. BOYNTON. Mr. Chairman, we used our intelligence fusion center—it is a State-run entity, one of 72 around the country—to disseminate that intelligence bulletin, and we did that in two ways:

First, for those who have security clearances, we provided a classified briefing. We have tripled the number of people in Connecticut, like police chiefs, with those clearances, and we are adding more.

And, second, with the unclassified part, our fusion center has an existing network to send that out quickly to every police department, and in this case, since it was not law enforcement sensitive, also to all first responders. And I should not say "police department," but all police partners, so that includes not only municipal police, State agencies with police forces, but also Amtrak and MTA within Connecticut.

I do want to add that part of our reaction from that intelligence took place a year ago and prior to that, that we have been doing things, in my view, that help us now, but we did not start now. And one example of that is getting that TSA intelligence analyst into our fusion center as a primary work site. What that allowed us to do is have someone already in place in that fusion center who we then could ask to focus on surface transportation, focus on rail, and we have already had two cases since then of potential rail tampering, of potential rail gate tampering in neighboring areas.

Chairman LIEBERMAN. Right.

Mr. BOYNTON. But through the collaboration between fusion centers, because we have the luxury of someone who focuses on that—but that is something that was in place 2 years ago, which helped us now.

Chairman LIEBERMAN. So was there an event that led to that occurrence 2 years ago, or was it an administrative decision at some level, TSA or State?

Mr. BOYNTON. It was an administrative decision between the Federal Security Director for TSA at Bradley Airport and the Commissioner of Homeland Security. It was the previous TSA Federal Security Director that——

Chairman LIEBERMAN. What was his name?

Mr. BOYNTON. I think that was Commissioner Boynton.

Chairman LIEBERMAN. Thank you. My time is up. [Laughter.]

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Pistole, I want to start with something that Dr. Flynn raised in his testimony. He said that the first rule is to avoid alienating the very public that security officials are obligated to protect. As you know, there has been some criticism of TSA over the years, most recently about the selection of a small child to be patted down, but also people have raised questions about why a very elderly woman had to go through such scrutiny.

Is TSA considering any actions that would focus more on a risk analysis using intelligence to select individuals for secondary screening?

Mr. PISTOLE. Thank you, Senator, and I agree with that point in terms of not alienating the public that we are trying to protect. The challenge, as we know, comes in the practical application of that. And to your point, we in TSA since last fall, actually before the Thanksgiving issues arose, have been looking at a risk-based security initiative to do exactly what you have described, to try to identify those that we know something more about, whether they are frequent flyers, whether they hold top secret security clearances, whether they, based on the intelligence we know, do not fit in a category such as the very young or perhaps the very old, who we could expedite their screening at airport checkpoints. That would then allow us to spend more time with those that we do not know very much about other than what is in Secure Flight, the three data fields, name, date of birth, and gender, which allows us to compare to the terrorist watchlist. We obviously want to spend the most time on those who would be selectees, but then in the next category, I would say we want to spend as much time as possible on those that we do not know much about and then the least amount of time, frankly, using a risk-based approach, to say this person has traveled 100,000 miles in the last year, she has done that for the last 20 years, what is the possibility of her being a terrorist? It is very small, so let us treat her in that regard.

So it incorporates some of the aspects of what is known as trusted travelers, known traveler programs, and some other aspects of that. So we have had a fair amount of discussions with industry about that. There is a great deal of interest, whether you talk about a checkpoint of the future that one association is promoting. There are a lot of technology aspects to it, but a lot can be done right now with enhanced behavior detection and information that passengers are willing to share with us.

Senator COLLINS. Thank you. I support TSA's and DHS's expansion of the See Something, Say Something campaign, and indeed, mass transit systems have been using this for many years. New York City subways, for example, have had it for nearly a decade.

I mentioned in my opening statement that Senator Lieberman and I authored the law to give immunity to individuals who make such reports, as long as they make them to the proper authorities and act in good faith. This was in response to an infamous case involving US Airways when passengers did just that, and then the airline, its crew, and some of the passengers got sued.

Does TSA or do you personally support extending the law so that it is not just confined to the transportation sector?

Mr. PISTOLE. Senator, I think it makes sense. We want to encourage people to provide information without concern about liabil-

ity from something that would come about. That being said, I know the lawyers at DHS are looking at all of that and are going to provide a formal response, but, yes, I think it makes sense.

Senator COLLINS. Thank you.

Commissioner, you have so much experience at the State level, and one comment that you made that really resonated with me is when you said that their security, the security of big cities, depends on our security, that you are feeding people into those lines. It resonates with me because two of the hijackers on 9/11 started their journey of death and destruction from Portland, Maine, and I think that is often forgotten when some of our colleagues argue that all of the homeland security money should go to just large urban areas. My colleague from Kentucky just had the case where two suspicious individuals in Bowling Green, Kentucky, were arrested. So I think that we need to understand in this country that security is everyone's business, that terrorists hide and train and plan in rural areas and not just in the areas that they are apt to strike. So thank you for making that important point.

I want to ask you about the training exercises. Like the Chairman, I have been a huge proponent of having more exercises that involve Federal, State, county, and local officials because if disaster strikes, you do not want people meeting each other for the first time and exchanging business cards in the middle of it, which is what happened with Hurricane Katrina, and that is why we restructured FEMA to have regional offices and have pushed and funded these training sessions.

I want to know from you, however, whether we are striking the right balance. CRS tells us that the transit security measures, including training, tend to emphasize managing the consequences of an attack. In other words, they are focused on response. And I agree with Dr. Flynn that response and resiliency are important. But to me, our focus should be on trying to detect, deter, and prevent the attack in the first place.

So how do you rate the effectiveness of the training sessions? Are we striking the right balance between teaching prevention techniques versus consequence management?

Mr. BOYNTON. Senator, I can tell you that we have had a number of exercises in Connecticut—Norwalk, Old Saybrook, and two other locations—and another one where we sent from Bridgeport about 40 people to the TEKS Program down in Texas, a terrific program where they do very well simulated exercises. And the unusual thing about this was that it included fire, police, emergency management, emergency medical—all four disciplines, including the chiefs from each of those departments—carving out essentially a week of time and moving 30 people down to Texas to do this. So it was a fully integrated training exercise. That was just within the last couple months that we did that, and the key thing there was the fully integrated part of it.

In the case of the exercise in Old Saybrook, which is on the northeast corridor, that included taking a rail car off on a siding and then simulating a shooting event, all phases of the response right to the point of actually taking passengers out through the windows. Normally something like that is simulated because you might hurt somebody in the exercise. They actually went to that

level of actually moving people out of the windows. So really terrific exercises, but I would agree with you that the focus is on response, and I think perhaps as part of this not just see something and say something but do something, that really could be a great trigger for us to then move into training and exercising not just first responders but some members of the public to help us with what specifically are we asking you to look for and how exactly are we asking you to report it, and then what do you do. And it is not that we have not done that. We have very robust See Something, Say Something campaigns, but I think we could use more in that area.

Senator COLLINS. Thank you

Mr. FLYNN. Senator, could I add just one thing to that?

Chairman LIEBERMAN. Go ahead.

Mr. FLYNN. One of the reasons why I place such emphasis on response and recovery is that it helps to get people vested in couldn't we do more to prevent something in the first place. In other words, when you get citizens involved in response and recovery, they become much more vested in how they could be helpful in prevention efforts. So exercises are so important because, as a practical matter, we are not going to eliminate every threat, which could lead us to overreact. But exercises also very much support prevention and protection efforts as well.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Dr. Flynn, and thanks, Senator Collins. Senator Paul, you are next.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Thank you, and thanks to the panel for coming today.

I wanted to follow up on Senator Collins' question to Mr. Pistole. Currently, the invasive patdown searches are random and not based on risk assessment?

Mr. PISTOLE. No, actually they are based on intelligence that we know specifically from Christmas Day, Abdulmutallab, and the way he concealed that device. There are some random patdowns, if that is what you are referring to, but it is based on the intelligence.

Senator PAUL. So I guess this little girl would be part of the random patdown? This is the little girl from Bowling Green, Kentucky, one of my constituents. They are still quite unhappy with you, and I and a lot of other Americans think you have gone overboard and are missing the boat on terrorism because you are doing these invasive searches on 6-year-old girls.

The same week that this happened, I received a call from another neighbor of mine in Bowling Green. A little boy had a broken foot and crutches. They did not want to go through all the screening, so they took the crutches off and the cast, and he wanted to hobble through on his broken foot, and his Dad was helping him. TSA said, "Back away. Back away." Then he had to go through the special search because he previously had a cast on even though the cast went through the belt. When the Dad comes close, they say, "Back away. Back away. If you do not back away, you will not fly." This kind of gets back to this whole idea of what are we willing to do, what are we willing to give up as a country.

In your interview with ABC News, you said, "I see flying as a privilege." Well, there are those of us who see it otherwise, the Supreme Court included, and *Saenz v. Roe,* in 1999, says that although the word travel is not found in the text of the Constitution, the constitutional right to travel from one State to another is firmly embedded in our jurisprudence.

Justice Potter Stewart went on to say in *Shapiro v. Thompson* that the right to travel is so important that it is assertable against private interference as well as governmental action, a virtually unconditional personal right guaranteed by the Constitution to us all.

Now, this is not to say we do not believe in safety procedures, but I think I feel less safe because you are doing these invasive exams on a 6-year-old. It makes me think that you are clueless since you think she is going to attack our country and that you are not doing your research on the people who would attack our country. It absolutely must involve a risk assessment of those who are traveling. The fact that she is being patted down—I do not feel comfortable really with your response that, "We are no longer doing it. We may be doing some risk assessment. We are still doing random patdowns." I think you ought to get rid of the random patdowns. The American public is unhappy with them. They are unhappy with the invasiveness of them. The Internet is full of jokes about the invasiveness of your patdown searches. And we ought to really just consider whether this is what we are willing to do.

While we are doing "random patdowns," there are examples where we have had letdowns. When Faisal Shahzad got on the plane, the alleged Times Square bomber, he was on the watchlist. Everybody said, "It was the airline that let us down." Well, he had to go through TSA screening. It was not a long time, but there were 10 hours, and we ought to be able to react. His name was on the watchlist, and he went right through TSA.

Is the TSA looking at flight manifests? Are you doing background research of people getting off and on planes? Are we targeting who we are looking at based on who might attack us? I really get the idea that because our approach is so politically correct, it has to be so universal that 6-year-olds and 90-year-olds and people in wheelchairs are agressively screened. You probably saw in the newspaper the other day the young man who is mentally handicapped who had a plastic hammer. Because you are telling your agents to do this, they took away something the boy had had for 29 years. If you have ever dealt with a child with autism, there are certain things that comfort them and keep them calm, and to do that really just shows that no one is thinking. They are given this rote, automaton message to crack down, pat people down, and do this. Catching terrorists should be about police work. Most of these people are caught by police work. The hijackers who came here were overstaying their welcome. They were on student visas, but they were not going to school. We need to be doing better police work and less of the universal giving up of our freedoms.

I would like you to comment a little bit about the right to travel as a privilege and then a little bit about the idea of the universality of insult that we are being given versus targeting this toward people who might attack us. Thank you.

Mr. PISTOLE. Thank you, Senator. You have raised a number of important issues. Let me try to take them in order.

In terms of the patdown of the 6-year-old, that, of course, is something that is done based on intelligence that is gathered from around the world, not as to a specific individual, but if there is an anomaly detected or for some reason the resolution cannot be done other than through a patdown, that is what is done. Unfortunately, we know that terrorists have used children under 12 years old as suicide bombers in other locations—not in aviation, but there have been two 10-year-olds used. We also know that two grandparents—one grandmother and one grandfather, 64 years old in both situations—have chosen to be suicide bombers. So it is informed by the intelligence.

I agree with you that we need to be smarter in how we go about doing things. We need to use more common sense. When TSA was stood up nearly 10 years ago, it was given a mission: Do not let this happen again. And the men and women of TSA have taken that very seriously. Secretary Napolitano and I are working on a risk-based security initiative to say, yes, let us take what we know, some of the passenger manifest information, especially those who are willing to share information with us, so we can make better judgments, better informed decisions as to this particular person, what risk do they pose? And so how can we expedite their screening if they are not seen as a risk?

So we are doing a number of things. I would be glad to provide some more detailed briefings to you in a closed setting on that.

Senator PAUL. Right. And just one follow up on that. I mean, 10 years is a long time. It has been a decade now. We do not have a frequent flyer program. We do not have a trusted traveler program. I do not want this to be against the TSA. I know most of the agents, and I think they are good people. But at the same time, they are wasting their time. All these Congressmen and Senators go back and forth, but to be fair, TSA agents have to search all of them. They know us by name a lot of times, and we are getting the same patdown search as everybody else to be fair. But so are the frequent travelers. My brother-in-law is on two or three planes a week. He is an Air Force graduate. He is clearly not a terrorist. And so they are wasting time on all these people. But I really think as far as the privacy issue, there were the beginnings of this, let us turn it over to a private company. We should have a frequent flyer program that you can voluntarily participate in. Let us get it done. Thank you.

Chairman LIEBERMAN. Thanks, Senator Paul.

I want to just clarify about the 6-year-old. Based on the evidence that children have been used by terrorists, did that 6-year-old set something off in the screening that led to the patdown? Or was it a random patdown?

Mr. PISTOLE. No, if I recall correctly on that particular one, the child moved during the screening so they were not able to get a clear reading. And so what we have done, just for your awareness, we have changed the policy to say that there will be repeated efforts made to resolve that without a patdown.

Chairman LIEBERMAN. Right.

Mr. PISTOLE. Although it is premature, I will be announcing something in the not-too-distant future about a change in policy as it relates to children and under.

One of the challenges, as you know, is that we not provide a road map to terrorists saying here is exactly the criteria.

Chairman LIEBERMAN. Right.

Mr. PISTOLE. And so if this category is exempt from most screening, then how will terrorists exploit that and game the system. So that is our challenge and that dynamic between security and privacy we try to tread.

Chairman LIEBERMAN. Thanks. Senator Landrieu.

OPENING STATEMENT OF SENATOR LANDRIEU

Senator LANDRIEU. Thank you. Mr. Chairman and Senator Collins, thank you so much for holding this hearing. I think it is extremely timely and extremely important.

As you know, I am the Chair now of the Appropriations Subcommittee on Homeland Security, and Senator Coats and I are in the process of writing our bill for this year, and this is a very important subject and very timely because, unfortunately—which is why I wanted to come this morning, to call to your attention since you and Senator Collins have worked so hard on the reorganization, the development and creation of the Department of Homeland Security, and have put so much effort into it—the homeland security bill that has been sent over by the House of Representatives cuts the exact grants that support rail and transit security and emergency response by over 60 percent. So I do not know how we accomplish the security objectives that are the subject of this morning's hearing with a 60-percent reduction in the grants—transit security, port security, training and preparation. This cannot be done on the cheap, and it has to be well resourced and well focused. So I wanted to bring that to your attention.

In addition, I want to also strongly object to the 35-percent cut in Science and Technology because, clearly, this is an area where we need more science, not less, and better technology, not mediocre or the same technology. We have to stay ahead of the terrorists, not behind them, and I think cutting a research and development budget borders on reckless, and we have received a bill from the House that comes 44 percent below the President's request for this year and 35 percent below where we were in fiscal year 2011.

Let me give you a specific example. The VIPR teams were described this morning as being highly effective, and the President included in his budget funding for 12 additional VIPR teams. Those have been eliminated in the House homeland security spending bill. So I want to submit for the record the rest of my statement in writing, but Senator Coats and I have quite a challenge to put a budget together that supports some of these efforts and the obvious and evident evolving threat, particularly since based on the information that we received from the capture of the documents from the Osama bin Laden compound, we now have not a direct but a

pretty good idea of where some of this was headed. So I want to just include that in the record.[1]

I do want to associate myself with the remarks of Senator Collins and the Senator from Kentucky. I think some of these patdowns of children—and I have expressed this to you before—are so contrary to what we are trying to accomplish, and I surely hope that TSA can be responsive and smarter about what we are doing.

The travel industry is very important to Louisiana—and to many places, but our State has a tremendous business and industry built on travel. We have been hearing a great deal from the industry about the difficulty, the loss of jobs, the loss of income, the missed opportunities to get travelers into our country because it is, frankly, getting so difficult to get here, people are choosing to go elsewhere. We want terrorists to go elsewhere. We do not want business people and tourists to go elsewhere. We want them to come to Connecticut and go to Maine and come to Louisiana and go to New York.

So what is your timeline for a trusted traveler program? Is there something that this Committee or the Appropriations Committee could help you with? Specifically, what is your timeline for some sort of trusted traveler program?

Mr. PISTOLE. Well, first, Senator and Madam Chair from the Appropriations Subcommittee, let me thank you for your supportive comments on the budget. Those items that you highlighted are key aspects of what we are trying to do in TSA and the Department of Homeland Security to protect the traveling public. So thank you for your strong support of that.

We are doing a number of things, and let me just briefly outline what we have done thus far in terms of doing a program with the pilots, those in charge of the aircraft, to say, look, they are the most trusted people out there. They are in charge of the aircraft. If they have a small knife or some prohibited item on them, frankly, that is not what is going to bring down the aircraft. So we have worked with the airlines and the Pilots Association to say, yes, let us go through identity-based screening with them.

We have also changed the policy for the World War II veterans who come into Washington, DC, to visit the World War II Memorial on charter flights. You know, the youngest of these——

Senator LANDRIEU. We have had the most honor air flights of any State, and I am so happy to hear that.

Mr. PISTOLE. So the youngest is 84, and two-thirds are in wheelchairs, and even though our officers are very respectful, talking about giving them a massage rather than a patdown, it is something that I felt was not needed, not common sense, and so we changed that policy several months ago.

Also, we are looking at children, looking at the elderly, and recognizing there are challenges there. And then to your point on the trusted traveler, we hope to be piloting some initiatives this fall to see how it would work. We are working with the airlines, U.S. carriers initially, to say for those willing to share information about

[1] The pepared statement submitted for the record by Senator Landrieu appears in the Appendix on page 440.

themselves, what can we glean from that that would help us make informed judgments?

Senator LANDRIEU. But do you have a timeline for the trusted traveler business flyers, not the pilots, not the Honor Guard, but——

Mr. PISTOLE. Right. So for the trusted travelers, whether we call them trusted traveler, known traveler, as I mentioned, we hope to start a trial this fall in select airports and airlines, U.S. carriers again.

Senator LANDRIEU. With the idea that if it goes well, we could implement it within 12 months or 24 months or——

Mr. PISTOLE. I would hope we would see some significant changes in 2012. I do want to make sure to manage expectations with the traveling public. It is a complex issue, and so I want to basically underpromise and overdeliver, but we will be doing some things that some passengers will see as early as this fall.

Senator LANDRIEU. I would hope that as you give pilots some access, you would consider also the flight attendants who work these long shifts and sometimes spend so much extra time in the airport that it just causes the morale of this whole industry to be at a level that I do not think is appropriate.

So I want to associate myself again with the remarks of Senator Paul and Senator Collins on this issue, and I thank the Chairman for his courtesy.

Mr. PISTOLE. Thank you, Senator.

Chairman LIEBERMAN. Thanks very much, Senator Landrieu. I appreciate your work on the Appropriations Committee, and I forget whether you were here, but I was talking about—what is the gracious adjective? I was about to say "foolish"—how foolish it is at this moment to cut the budget of the Science and Technology Directorate of the Department of Homeland Security. These are really investments in our future security. We all know we are under economic stress and we need to do things we would not normally do to balance the budget. But thanks for that and thanks for fighting for the other funding that you are fighting for, which I am confident will certainly lead to a higher level of support for homeland security than exists in the House budget.

We will do a second round of questions. Dr. Flynn, I missed talking with you on the first round. You are a very interesting and thought-provoking thinker on these subjects. You said a couple of things in your opening statement about both moving beyond screening, if you will, in these kinds of security matters and avoiding alienating the public that we are trying to protect. I want to ask you to talk a little bit more about that, particularly about moving beyond screening. I have assumed that we are doing screening of airline passengers because we cannot figure out, frankly, a more effective way to make sure that somebody does not go on a plane with the intention of doing harm, of carrying out a terrorist attack. And sometimes people have been before this Committee and asked a reasonable question, which is: We know it would be inconvenient to do airline-type screening on rail travel, but would we not feel more secure if we knew that everybody had been through some kind of detector to get on a train, particularly knowing that trains have been a target of terrorists?

I want to invite you to speak in a little more detail, to explain what you meant about moving beyond screening, and also perhaps to get into this question of what are the alternatives to screening. Are they as effective? And particularly with regard to rail, are there other things we could do, including more screening?

Mr. FLYNN. Well, Senator, thank you very much. I want to say first that, no matter what, screening is always in a portfolio of tools, but really per this conversation that preceded your question, one of the things that I am concerned about, the broad message that I think we need to take away from mass transit security, is you really need to make the public a partner in the process. And the face of homeland security for the overwhelming majority of Americans is what they experience at airports.

Chairman LIEBERMAN. Right.

Mr. FLYNN. And to the extent that they do not understand what is happening is being based on sound judgment, assessment of risk, and so forth, they are not likely to be cooperative. And so that is why I think we really need to speed up efforts to figure out how we do a risk-based screening approach, less intrusive for some portion of the population, and so forth. That is going to be very important, I think, for the broader effort.

But, the essential problem of relying heavily on a screening approach is that it largely assumes that everybody who enters the system poses a threat unless they can be discerned by a security official that they are not. And that is not manageable within the mass transit systems for them to work in most urban areas because it is such a time-sensitive, open system.

Chairman LIEBERMAN. Right.

Mr. FLYNN. As a practical matter, people know that they are taking risk on any system. There are safety risks, of course, associated with it, whether it is risk of personal safety in a busy station, people taking hazardous objects on trains, and so forth. They have to balance that with the function that they are trying to do, which is to get from A to B through that system.

The extent to which we get the public to be seen as both helping on the prevention side, aware of the environment, and everybody from the T-shirt vendors, as we saw in Times Square, the shoeshine boys, and others to be on the lookout for what we know are core elements of carrying out an attack—surveillance. Typically, nobody just shows up for the very first time to do something bad. They want to check out the place first because they need to be successful. There are typically dry runs that have to happen before somebody launches an attack.

All that creates opportunity for detection that this is somebody who is really up to no good, but also creates a deterrent for that person to come into that space because he is aware there is that operational kind of awareness and there is that engagement by the people who are present at the front lines literally, the passengers, the transit operators, the folks who are working around the station.

So the extent to which we emphasize screening at the cost of those engagement efforts, I think what you will end up with is alienation without perhaps the benefit that these other strategies would provide. And, again, we know in the case of aviation there is a portion of the public, the frequent-flyer public and people of

certain backgrounds, that we should be able to mitigate how much screening we subject them to, it should be a no-brainer.

We also need to give more discretionary judgment capabilities to screeners to make the calls versus to work in a real mechanical way. But, fundamentally, it is about getting the public more involved, and if they sense that this is solely the job of external screeners to do this and they do not have an obligation except to submit to the screening, then we are not going to get the kind of buy-in that I think we need about how to manage the risk going forward.

Chairman LIEBERMAN. That helps me understand. So you are not saying end screening. You are saying it has to be part of a total approach, and it ought not to be seen as basically giving the public a pass.

Mr. FLYNN. Yes.

Chairman LIEBERMAN. I think Dr. Flynn's insight about the people who essentially work and live in train stations is an interesting one, and I just wonder whether that is part of our normal routine. In other words, are train stations and transit systems training the news stand operators, the people at the coffee stands, the shoeshine people, etc.? Because they really do see a lot, and therefore, they can say a lot and do a lot.

Mr. PISTOLE. There has been a limited amount of that done, but we would like to expand that, as Dr. Flynn mentions.

Chairman LIEBERMAN. Good.

Mr. PISTOLE. I think there is a great force multiplier available to which we can avail ourselves.

Chairman LIEBERMAN. There is. I know that in air travel, of course, we do not just have the screeners, but we have people who are experts in evaluating the behavior of people boarding the planes. Since the consensus seems to be that because of the openness, the speed of the trains, etc., that we cannot and should not apply a screening model from aviation to trains, should we be using more behavior experts to evaluate people as they move onto trains or subways?

Mr. PISTOLE. Mr. Chairman, I think that is a good idea that we have been able to do on a limited basis. One of the key aspects of the VIPR teams that we use with random and unpredictable aspects is to not only have this uniform presence because we know that terrorists are deterred by uniformed law enforcement officers, K–9, and CCTV, unless they are a suicide bomber then they do not care about the CCTV. But those three things are important layers of security all informed by intelligence. But when it comes to behavior detection, one of the best opportunities we have is when there is a VIPR team, let us say a dozen uniformed officers, K–9, walking through a train station, to have a plainclothes behavior detection officer to see people responding to that. I would have loved to have been in Schiphol Airport on Christmas Eve 2009 to see Abdulmutallab walking with his underwear bomb toward screening and to have a K–9 uniformed officer walking toward him, then with a plainclothes behavior detection person observing how does he respond to that officer and that K–9. I doubt that he would have had the audacity to walk right by that person, the K–9, for fear of detection.

Chairman LIEBERMAN. Right.

Mr. PISTOLE. So that is what is key: How can we deploy behavior detection in a smart, efficient way? We are not currently budgeted to do that across the board, but that is how we try to be force multipliers to State, local, and Amtrak.

Chairman LIEBERMAN. Very smart. That combination I think would be very effective. Thanks. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Pistole and Commissioner Boynton, I listened to the exchange with Senator Landrieu, and I, too, am concerned about the deep cuts in some of the homeland security grant programs. One challenge that we face, however, is that there has been a low rate of obligation of the money in the area of mass transit. And, indeed, there was one audit that was done by FEMA—and I realize these are FEMA grants, so if you cannot fully respond, I understand. But back in fiscal year 2006, something like 90 percent of the money for mass transit and rail security measures remained unobligated.

Mr. Pistole, are we doing better in getting those funds out? And, Commissioner Boynton, from the local level or from the State level, can you give us any insights on why it takes so long for that money to actually be expended for the purposes of improving security?

Mr. PISTOLE. Thank you, Senator. Let me start off by saying, yes, we are doing better, but we are still not where we should be in terms of the whole process. It is something that I think has frustrated everybody involved. You have correctly identified that TSA is responsible for identifying with FEMA and DHS and the industry where the highest risks are and for awarding the funds, and then the actual drawdown of those funds and the use of those funds are up to, obviously, industry and FEMA how that works.

Some of the issues, I think, going back to 2006, were with multiyear projects that were, if you want to say, not shovel-ready, if it came to actually critical infrastructure enhancements and things, whether it is strengthening tunnels or bridges and things like that. And so I think there has been additional focus on operational deterrence things, such as training where even though there is still delayed rulemaking that is out there, over 90 percent of the people in the critical high-risk transit areas have been trained. So even though the rulemaking is still pending, we have gone ahead and provided the substance of what was to be covered by the rulemaking. So we are not letting the bureaucracy, if you will, get in the way of the substance of what, in this case, the 9/11 Commission Act required. I will defer to Commissioner Boynton on the other parts.

Senator COLLINS. Commissioner Boynton.

Mr. BOYNTON. I think I can give a couple examples. In one case, we have a capital improvement project on the Metro-North Line where we want to put fiberoptic cable along the entire line to connect all of the CCTV cameras. We have cameras at a number of stations, different places along the line, in the rail yards. Right now most of those cameras—not all of them but most of them—are localized. And given the governance of the rail system, that can be problematic, and let me just give one example.

There are towns along the rail line where there are multiple stations in the same town, and each one of those stations is managed

differently by different entities, some with participation by the municipality, even within the same municipality, some without. So tying these cameras together is very important to us. We are unable to compete, given the size of our transit system, to fully fund the project at any point in time. So the best we have been able to do—since 2006, we have just over 1.5 percent of the national total of transit security grants—is to save the money to get the project done. We think we have saved about half. In the meantime, we are moving ahead with the design phases of the project with additional cameras. We are holding the money on purpose because we cannot afford the project in any 1 year because we are not able to compete at that level. And I am actually not being critical. The needs of the much larger transit systems in the large urban areas are overwhelming. I want them to have more money than we have, but part of the reason we are holding that money is on purpose. And then there is a second reason, and it is not just the transit grants. It is many of the other grants in our grant portfolio. Many of these grants have 3-year performance periods. Those are the rules we were given. In all of our grant planning with, in our case, 169 municipalities, two tribal nations, dozens of State agencies, we were told, "You have a 3-year performance period for these grants." We have statewide homeland security strategies, 10 goals, 80 objectives, 403 measurable criteria, all laid out. We have 3 years to spend this wisely. It is coming as a little bit of a surprise to us now that we are being challenged: Why have you not spent this money? We have not spent it because we were told we had 3 years to spend it, and we are using that time wisely.

Senator COLLINS. Dr. Flynn, do you have anything to add to this? I know it is more the other two witnesses' purview.

Mr. FLYNN. Sure. What I continue to hear about is the difficulty often of chasing these very small numbers of dollars, so I guess I would just reinforce the concern of Senator Landrieu that some folks basically saw there was maybe a pot of gold that you would have in Washington to advance homeland security at the State and local level and through critical infrastructure. I often characterize it as a "thimble of gold." And what happens here is these decisions are being made in a kind of triage fashion. At its core we have to look at these as systems.

I think one of the important points that Commissioner Boynton made here today is about how the riders who are coming from Connecticut as far away as New Haven, 90 miles, are going to the belly of the beast, Grand Central Station in Manhattan. And assessments about where we apply resources and how we roll them out, that is going to take time. It is not something you can just throw together. You have to have the collaborative mechanisms. And I want to reinforce the idea of using the area security committee model we have in the maritime world as potentially a process for managing grants in the other transportation sectors. It is very important, and we often lose sight of this. In the case of Connecticut, trains connect passengers to ferries. It is trains, buses, and trucks, and it is all there together. And connections by trains to airports, such as Newark Airport.

We have not really been looking at the system and the integrated nature of that system, leaving State and local officials to fight for

scraps, and the scraps are not being used as well as they should be used.

Senator COLLINS. What worries me—and, Commissioner, I am going to use your examples—is many of our colleagues look and see unobligated funds, or funds that have been obligated, but it is 2 years later and they have not been spent, and they make two conclusions: The program is overfunded, that money was never needed in the first place, we can slash that from the budget; or they conclude that it is being poorly managed and is not really needed, and thus, they reach the same conclusion that it can be slashed from the budget.

The desire around here to sweep up unobligated or unspent funds is enormous, given the budget constraints, and the irony is that it penalizes projects and good planning and communities that are actually spending the way you would want them to spend. They are formulating a careful plan so that they do not waste the money. And I think this is going to be a real battle for us. I hear it all the time from our colleagues, "Well, the money is not needed because it has not been spent," when, in fact, the careful planning that is going on, which takes time, ensures that the money is spent wisely and not wasted. But it is an uphill battle, I will tell you.

Finally, Administrator Pistole, I want to commend you for keeping your commitment made a year ago to come up with a Surface Transportation Security Priority Assessment. For the record, I would like you to give us an update on the 20 recommendations that you made as far as what the timeline is for implementing those recommendations and how it is going. But I do commend you for completing the project.

Mr. PISTOLE. Thank you, Senator.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

I would just indicate to the witnesses, in the characteristically unpredictable way the U.S. Senate works, we are not taking up a bill on the Senate floor at 11 a.m., so we have a little more time.

Senator Carper, thanks very much for being ready to take the gavel if Senator Collins and I had to leave, and thank you for being here now to ask your questions.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you. I apologize for being in and out. We have a Finance Committee hearing going on just one floor below, and we are focusing on improper payments or overpayments of about $17 billion a year on unemployment insurance. So that is important. This is important, too, and I tried to go back and forth as best I could.

I just want to mention that for about 8 or 9 years, Senator Biden and I used to ride the train together, a lot of days back and forth, and before that with Mike Castle, our Congressman. And I still ride the train almost daily now with Senator Chris Coons and with Congressman John Carney. I call us "The Three Amigos." We love to be able to live at home and take the train to work.

Every morning the train is packed with passengers. In fact, I sat in the quiet car this morning. Every seat was filled. And I think Amtrak has set a record again this year. I think last year it was

about 28 million. This year they are, I think, approaching 30 million people. And I am delighted that so many fellow Americans have decided to take the train along with the rest of us.

However, I am also concerned about the threat that those 30 million passengers face, as well as others who ride the rails with local transit services. I just want to ask how the Department of Homeland Security is coordinating with Amtrak to improve train safety. Mr. Pistole.

Mr. PISTOLE. Thank you, Senator. We work very closely with Amtrak. Chief O'Connor and I speak frequently about security precautions that they take unilaterally and best practices that we recommend from either here in the United States or from around the world. We have provided Amtrak nearly $100 million—$97 million since 2006—for specific security enhancements to Amtrak to protect those 28 to 30 million people who are traveling every year, and there are a number of aspects to that, both on training of Amtrak officers and rail personnel to look for anomalous activity, obviously the See Something, Say Something campaign for the general public, the ridership especially, and enhanced K–9 patrols

Senator CARPER. Do people ever say anything? When I am at Union Station and the station back home, I hear these announcements all the time. You hear them in airports, too. But do people ever say anything?

Mr. PISTOLE. Yes, in fact, I have asked that question because we are investing in that, and the answer is yes, in some places more than others. One example I have is in Boston from the MBTA where from 2010 to 2011 they have seen over a 100-percent increase in people reporting things. Now, they have taken some interesting initiatives, including one of which I happen to have a photo of a 16-foot or 12-foot backpack that they put out in some of their stops, and Chief Paul MacMillan is standing by that backpack, and the caption is: "It is never this obvious." So it is not going to be a bomb that just looks like something huge like that.[1]

Senator CARPER. The folks in the audience cannot see that. That is a big backpack.

Mr. PISTOLE. That is a big backpack, right.

Senator CARPER. I would certainly say something if somebody came carrying one of those on their back.

Mr. PISTOLE. Yes, so the idea is it is not as obvious as that, so let us be alert, let us be attuned to what is around us, and I think the partnership, which was mentioned on the panel this morning, is the key criteria. So we can do all the security enhancements, we can do all those things, but I think it really will come down to an alert individual, perhaps a police officer, or perhaps a K–9, who sees something and takes action to disrupt a possible plot.

The best opportunity we have is like what we saw with Najabullah Zazi where we were informed by intelligence well before he got to New York City with the backpacks. That is the best possible opportunity we had. Or, for example, the Yemen cargo plot with the toner cartridges, intelligence that helps inform our judgments. If it gets through all those layers of intelligence and somebody is actually getting on a train in Wilmington or Newcastle or

[1] The photo referenced by Mr. Pistole appears in the Appendix on page 449.

wherever, and we know nothing about them, then it really comes down to somebody seeing something and taking some action with local law enforcement or Amtrak.

Senator CARPER. All right. Thanks.

Mr. Boynton, as a State partner, you have, I think, an interesting perspective on the interaction between Federal, State, and local security officials. Many of the public transportation systems that service Connecticut also travel through other States, such as Amtrak and the Metro-North railroads. These interconnected systems require coordination among multiple public safety agencies, as you know. Are we doing an especially good job of functioning well together? And how can that be improved?

Mr. BOYNTON. Senator, we have a couple forums, and I like to tell people that what we do is we provide a table and ask people to come to the table. We have created a transit security committee with representatives from every mode—trucking, bus, maritime, aviation, pipeline, highway, rail, all of them. And what we found was, all of the rail people know each other. Same with the bus people. We think they may never have been in the room together before, however.

Senator CARPER. How do they get along?

Mr. BOYNTON. Well, it is clear that they are all out of their comfort zone, actually. We have all heard about people operating in silos, and one of those partners, just in the last few weeks, used a term I had not heard, which was "cylinders of expertise." They are all very good at what they do. It requires effort to bring them to the table, and the first time we met, we saved $60,000 in the first 10 minutes. The rail people were talking about a See Something, Say Something campaign, and the bus people said, "We are working on a campaign. Can we use yours?" And the answer was yes. They saved $60,000 in about 2 minutes. They both worked for State government. They both worked in the same department of State government. But they were all within their comfort zones, so this collaboration that the Administrator speaks about, it is absolutely key. This is one way we do it. The other way we do it is with our fusion center. We have a full-time TSA analyst whose primary work site is in that fusion center.

I find examples like that to not necessarily be the norm. I find that the agencies we work with do a lot of great work, building capacity and building expertise, but trying to get people at the same table and to stay there as primary work sites while not exactly hard to do, takes a special focused effort. And once you do it, you cannot stop. It has to be sort of continual to keep people at the table because, by definition, it is out of their comfort zone. They are not with their parent agency.

Senator CARPER. All right. Thanks. Mr. Chairman, could I ask one other question?

Chairman LIEBERMAN. Go ahead.

Senator CARPER. I understand, Dr. Flynn, that in your written testimony you provide compelling evidence of the deficiency of rail and transit security. I think you may have mentioned in your written testimony that roughly $9 is spent for safety on every airline passenger, and we spend about one penny per rail and transit pas-

senger. How can we use limited resources to improve the Federal Government's existing transit and rail security programs?

Mr. FLYNN. Well, Senator, thank you very much for the question. The case I tried to make in my testimony and advance is that there actually are some relatively modest things versus very expensive things that we can be doing, some around, just as we are covering here today, the focus on public education efforts. I mean, if you ask a law enforcement agency to develop the message of See Something, Say Something, it is going to come out a little differently than maybe talking to some folks out in Hollywood who will come up with a different idea.

The big backpack I think is a wonderful illustration of reaching out to real talent pools that exist, but that takes some resources to be able to go out and say: "Here is a message we are trying to convey. Can you help us with this message? Because you know what people will listen to and pay attention to." So that is an investment that raises awareness that hopefully makes sure that we can prevent things by taking advantage of all those eyes, the 28-30 million on Amtrak trains. We are not going to get all of them, but we could get more than relying on a lot more dogs or a lot more—and, again, not either/or but a huge multiplier by taking that transit public who is with the rhythm of that train and knows the train station and gets them involved there.

The other, it takes funds to be conveners, and I guess I would push a little bit. I think what Connecticut has done is a model, but it still is largely intra Connecticut—as opposed to efforts that reach beyond the State. It is very difficult often to get the States to play well with each other, something that I know you have some experience with here, because everyone is fighting for so few resources. And so to the extent to which these area security committees, regional committees, and so forth really bring key players together, they can build on what is a superb State initiative, but make sure there is something like that going on in the surrounding area so people can recognize that See Something, Say Something for the buses that Connecticut is doing could be done also in Delaware.

The challenge is that you cannot get to homeland security without really dealing with the horizontal, and the horizontal is dealing with the citizens, the private sector, the community, State, and locals. But we are still coming at it vertically and/or episodically, like spitballs on a map, a few major urban areas, let us try to fix some of those. And this lack of a holistic approach I think is a serious problem. I am very worried about the budget climate reversing the few embryonic steps that we have made to achieve the horizontal, engage the public a bit more, draw them on board. And if we lose ground on the science and technology front and so forth, it will take us years to get back to where we want to go. And God forbid we have the next major event and people see that we essentially stopped working on the problem and stopped making modest investments.

Senator CARPER. Mr. Boynton.

Mr. BOYNTON. Senator, could I just comment on one point there?

Senator CARPER. Sure.

Mr. BOYNTON. The difficulty of communicating between the States, I have seen over the last year, 18 months a really encour-

aging increased ability for the fusion centers to talk among each other. These are all 72 fusion centers, State or locally led, with the Federal participants but an increasingly good dialogue between these fusion centers, and that helps us with the regional approach and across-State approach.

Senator CARPER. All right. I am glad to hear the kind of communications you all have started up in Connecticut. That is the kind of stuff that we do in Delaware. I am proud of it. Thank you.

Thanks, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Carper.

Thanks to the three witnesses. I think you have been very helpful. I am reassured from this hearing that there has been a response to the evidence that came out of Osama bin Laden's compound about potential attacks on mass transit systems in the United States on or around September 11 of this year. I appreciate the continuing work that is being done. We are up against an enemy that is not smarter than we are, but is certainly more inhumane and ruthless than we are. To say the obvious, with regard to the discussion with Senator Paul about patting down a child, unfortunately there is an evidentiary basis for doing that, which is that some of these terrorist groups have used children and have been willing to risk or take their lives as a result, and they have used grandmothers and grandfathers to do the same.

So when you are up against this kind of enemy and we are attempting to maintain freedom of movement in our country and the openness of our country, it is not easy. So I share the sentiment that has been expressed across the panel, which is that we have to be very careful as we cut budgets that we do not take big risks with our security because in the end that really is the first responsibility of our government.

I thank each of you for what you are contributing to homeland security. We are going to leave the record of the hearing open for an additional 15 days for additional questions and statements.

With that and the Committee's gratitude, I hereby adjourn the hearing.

[Whereupon, at 11:26 a.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11: PREVENTING TERRORIST TRAVEL

WEDNESDAY, JULY 13, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Collins, Brown, and Paul.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Normally I am a few minutes late and Senator Collins is on time. Today she surprised me, but she is in the hallway, so I will take the—there you are. I was just saying you are normally the more punctual one—it is not really an odd couple relationship we have—so I waited a moment or two.

Senator COLLINS. I apologize.

Chairman LIEBERMAN. Not at all.

I want to welcome everyone to this hearing, which is the fifth in a series of hearings that our Committee is holding this year to review the state of our Nation's terrorist defenses as we approach the 10th anniversary of the attacks against America on September 11, 2001.

Denying foreign terrorists the ability to travel to our country to attack us, as they did on 9/11, obviously is a continuing homeland security priority, and that is what we are focusing on today.

As you look back over the 10 years and think of all that we have done to meet the challenge of preventing terrorists from coming into the country, you have to say that, thanks to a lot of people, we have done very well at it. There has not been another major attack from outside. And yet there have been attempted attacks in which people have certainly shown they are still trying to enter the country, or succeeded in doing so, such as the cases of the shoe bomber, the Christmas Day bomber, and the Times Square bomber. All plotted outside the United States with help from al-Qaeda and other Islamist terrorist groups, and all involved travel into the United States.

In the years since September 11, 2001, legislation authored by this Committee has created a number of programs and systems meant to enhance our government's ability to identify and stop terrorists among the millions and millions of people who travel to the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00133 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

United States and who we want to welcome each year. The terrorists, obviously, we want to prevent from entering our country.

The Homeland Security Act, which created the Department of Homeland Security, gave the new Department the authority to set visa policy and deploy Visa Security Units to overseas consular posts, working with the State Department to provide an added layer of security in the issuing of visas.

The Intelligence Reform and Terrorism Prevention Act of 2004, which was the original 9/11 Commission recommendations implementation legislation, called for a biometric entry and exit system for travelers into and out of the United States, and also required enhanced travel documents. It required consular officials to conduct personal interviews with all visa applicants.

The 2004 Act also directed the President to negotiate agreements with other nations to share information on lost or stolen travel documents. And perhaps most important, it required that domestic and international airline passengers be screened against terrorist watchlists.

Then the Implementing Recommendations of the 9/11 Commission Act of 2007, in a way the 9/11 Commission Act 2, created the Electronic System for Travel Authorization, a program that allows the Department of Homeland Security to screen travelers from so-called visa waiver countries against our intelligence and law enforcement databases before they board an airplane bound for the United States.

These programs are all critical new components of our post-9/11 efforts to deny terrorists entry into the United States. And I would say, looking back, for the most part they have been successful. But as is documented in a series of reports from the Government Accountability Office, we clearly still have work to do.

First, some good news: GAO reports that the Electronic System for Travel Authorization has been well implemented on our end and is helping to address gaps in the Visa Waiver Program.

In the same report, however, GAO says that only half of the visa waiver countries have signed the biometric law enforcement information-sharing agreements required for participation in the program, and none—not one—of these agreements has actually been implemented. So I would say today, looking back and forward, we really have to get them all signed and implemented as quickly as possible.

The implementation of the US–VISIT entry system has really been one of the biggest success stories of our post-9/11 efforts. It ensures that almost all non-U.S. citizens coming to the United States have their fingerprints registered and checked against all of our intelligence, immigration, and law enforcement databases prior to being admitted to the United States. That is a very significant filter, if you will, set up to stop terrorists from coming into the United States.

Unfortunately, implementation of an exit system has been one of our biggest failures. GAO recently reported to this Committee that US–VISIT's current biographic system has a backlog of over 1.6 million records of potential overstays that have not been reviewed. In other words, these are people who have entered America legally but overstayed the time during which they were legally authorized

to be in this country, and they become a very significant percentage of the millions of so-called illegal immigrants or undocumented aliens who are in our country. And this backlog is growing every day.

Tom Kean and Lee Hamilton, the co-chairs of the 9/11 Commission, in testimony before our Committee a few months ago, reiterated their call for a biometric exit system, and I would like to hear from our witnesses today about the current plans at DHS for getting this done because this really is a problem, knowing when people who come in legally are still here illegally.

I also continue to be concerned with the slow implementation of the Visa Security Program. Although the Department of Homeland Security and the State Department have identified 57 high-risk consular posts abroad, only 14 of them have criminal investigators to provide an added layer of security to the visa-issuing process.

The attempted Christmas Day bomber attack highlighted the importance of having adequate security measures in place at our consular posts, as you remember from that fact situation. But despite pledges by the Department of Homeland Security and the State Department to continue expanding this really important security program, the President's budget included no additional funding for this program for fiscal year 2012. Even in these obviously tight budgetary times, this is disappointing.

GAO released another report yesterday that found a lack of coordination and focus in our government's efforts to help our foreign partners develop their own terrorist travel programs, and that is something I am sure we will want to talk about today.

Finally, many of us on this Committee, particularly Senator Paul, who is here today, are concerned about security gaps in the Iraqi refugee program that allowed two Iraqi nationals, who turned out to be terrorists—one whose fingerprints were on an unexploded improvised explosive device that the FBI had in its possession from our troops in the field since 2005, so one of the two Iraqis arrested in Kentucky for planning terrorist acts actually had his fingerprints on this unexploded IED that was in the possession of the U.S. Government for over 5 years and was not processed in the system. Therefore, when this individual had his fingerprints done when he entered as part of the US–VISIT program, it was not correlated against this very implicating fingerprint that was in our possession, and so he was allowed to enter the country and then plot to send weapons back to their fellow terrorists in Iraq to use to attack American troops there.

We really need to know how these two were allowed to enter our country and why those fingerprints from 2005 have not been entered into our system. Senator Paul has focused the attention of this Committee on this matter, and I am sure he will have questions for the witnesses about it.

In sum, looking back, I think we can say with some satisfaction that we have made progress in the past 10 years toward making the entry by terrorists into the United States much more difficult than it was on 9/11/01. But we have also had some very unsettling experiences that show they can still penetrate the defenses that we have set up. And, of course, we know that they are adapting their mode of operating to our increased security measures.

Just last week, we saw published reports that al-Qaeda in the Arabian Peninsula is apparently at least considering if not carrying out the surgical implantation of explosives inside the body of an individual, which would be undetectable by most of our screening devices, but I will say clearly not undetectable by all of our defenses. Given these threats and their development, we have to continue to focus on this area of our homeland security, and that is our intention today. I thank the witnesses for being here. They are all perfectly positioned to report to us and answer our questions, and I look forward, after their testimony, to that part of the hearing.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Limiting the travel of terrorists is a key way to protect our country. As the 9/11 Commission put it, "Targeting travel is at least as powerful a weapon against terrorists as targeting their money."

According to the 9/11 Commission's report on terrorist travel, as many as 15 of the 19 hijackers might have been intercepted by border authorities if procedures had been in place to share intelligence data. At the time, however, threat information-sharing systems and policies were largely absent, and the hijackers' past terrorist associations were not readily available to American officials who could have acted.

Today, as the Chairman has pointed out, we have a more rigorous system at high-risk consulates to help identify those who should not receive visas, but we need to upgrade the Visa Security Program so that it can operate more effectively and in more high-risk posts.

This program deploys Immigration and Customs Enforcement agents to our high-risk embassies and consulates overseas to help identify suspected terrorists and criminals before visas are issued. The problem is that the United States has these offices at only 14 of the 57 high-risk posts.

It is also troubling that the GAO has found ongoing turf battles between ICE and the State Department's diplomatic security at some posts. VSP must implement effective procedures to help DHS and the State Department resolve questions about who should and who should not receive a visa to come to our country. All of those involved in the visa process at these high-risk locations must be rowing in the same direction for this program to reach its full potential.

There are other serious challenges and gaps in our security. As the Chairman mentioned, recently we learned that terrorists intent on attacking America have shown an interest in having explosive devices surgically implanted in their bodies. Yet a young man was able to fly cross-country from New York to Los Angeles without a valid government ID and with an expired boarding pass that was not even in his name.

At the other extreme, it troubles many Americans to see TSA putting the very young and the very elderly through intrusive and, in most cases, what appear to be unnecessary patdowns. If we continue to give extra screening to individuals who pose no threat yet others who should arouse suspicion can bypass checkpoints without

being questioned, our systems clearly are still not properly calibrated.

As Senator Paul will undoubtedly discuss today, and as Republican Leader McConnell and our Chairman have all highlighted, we also need to scrutinize the criteria for granting asylum. In May, two Iraqi refugees living in Kentucky were indicted on Federal terrorism charges. That they were permitted to come to this country on humanitarian grounds is shocking. How could this happen when there was sufficient evidence of the terrorist attacks in which they were involved to indict them? What is being done to close this serious vulnerability? Is the Administration re-analyzing the backgrounds of other refugees granted asylum under what appears to be a flawed process?

On the other hand, the *New York Times* today reports on cases of apparently worthy applicants who are not receiving asylum. Clearly, our system needs to be adjusted to ensure vetting and careful scrutiny so that those who are in danger of their lives because they have truly been allies of the American forces can receive asylum, but those who have been involved in attacking our troops or working with the Taliban or al-Qaeda do not receive asylum.

Even with improvements in our own safeguards, the United States cannot go it alone. Our intelligence reform legislation, which became law in 2004, directed the National Counterterrorism Center to establish a strategy to combat terrorist travel, and part of that strategy, an essential pillar, was helping to enhance the capacity of other nations to combat terrorist travel.

A new GAO report provides an update on our progress. While the United States has many programs to help our partner nations improve their visa issuance and screening protocols, the GAO has found that too often these programs lack coordination. The GAO also found redundancies. In one case, the GAO discovered that DHS and the State Department were both planning to hold training on fraudulent travel documents for the same Pakistani agency during the same month without knowing of each other's plans.

These programs, in my judgment, also do not focus sufficiently on corruption in the passport issuance process overseas, which, according to the GAO, is a significant obstacle in our efforts to keep terrorists from traveling.

There is, as the Chairman has mentioned, encouraging news as well as problems. DHS, for example, reports that nearly 450 suspected terrorists that were identified on a watchlist were blocked from boarding overseas flights bound for the United States in fiscal years 2010 and so far in 2011. The Customs and Border Protection is now matching passenger manifests with terrorist watchlists and not just with the no-fly list. It is vital to review these lists before departure and not once the plane is airborne.

Terrorists clearly are going to constantly probe our defenses and constantly innovate. Therefore, we must never cease our efforts to keep terrorists from acquiring the documents and the means to travel to our shores.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

Unfortunately, I just heard off the wire, just to show us how timely all this is, that at least three bombs went off in different

public places in Mumbai today, and this is just the first report. They are reporting many injuries. No indication of responsibility yet.

We have a vote around 10:40 and we will have to break at that point, but let us see if we can get at least some of the initial testimony in. I again thank the witnesses for being here.

We will start with Rand Beers, who is Under Secretary, National Protection and Programs Directorate, at the U.S. Department of Homeland Security.

TESTIMONY OF HON. RAND BEERS,[1] UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BEERS. Thank you, Mr. Chairman, Senator Collins, and Senator Paul. I am pleased to be here before this Committee which has been so important in the efforts to protect the homeland.

Our goal here in this area is to push information to the front lines, as Senator Collins and Senator Lieberman both indicated, as quickly as possible to prevent known and suspected terrorists from traveling to the United States. Today, I am testifying in two capacities—first as the Under Secretary for the National Protection and Programs, a position to which I was appointed by President Obama and confirmed by this body in June 2009, and am thereby responsible for the US–VISIT Program. I am also testifying today as the Coordinator for Counterterrorism at the Department, a role Secretary Janet Napolitano assigned to me following the December 25, 2009, bombing attempt on Northwest Flight 253. So what I will do is address what the Department is doing to better coordinate and prevent terrorist travel, describe the specifics of US–VISIT activities being done in this area, and also discuss my role as the Counterterrorism Coordinator.

DHS collects and screens information on who is entering the country or boarding an aircraft in order to identify possible links to terrorist activity. In this regard, the Department has made considerable progress since 9/11 to implement measures to identify and stop terrorist travel in five general areas:

First, unifying immigration and border management systems so that we can have the capability to access efficiently and effectively biometric- and biographic-based information across the entire homeland security spectrum.

Second, enhancing capabilities for more effectively identifying fraudulent documents and impostors and implementing measures to confirm document authenticity and validity.

Third, establishing a system of interoperability and information sharing that allows Federal partners across the government to share that information in order to do a better job identifying those persons of interest and concentrating on them.

Fourth, streamlining the visa overstay review process to establish reliable data on individuals who have violated the terms of their authorized admission.

And, fifth, establishing and maintaining strategic partnerships with an increasing number of international partners, sharing ap-

[1] The prepared statement of Mr. Beers appears in the Appendix on page 499.

propriate information, providing technical assistance, and developing commonality in biometric standards and best practices while investigating and testing emerging multimodal biometric technologies.

With respect to US–VISIT, let me just identify a few of the things that I think we have been doing. It is a broad program with important applications ranging from screening foreign travelers to immigration adjudication to law enforcement.

Interoperability and information sharing between agencies and international partners continues to yield significant results, as demonstrated by three success stories that I want to briefly mention.

The first occurred in February of this year. Australia sent us a batch of fingerprints as part of our High Value Data Sharing program. Within that batch we had a match on an individual about whom we had some terrorist information. We provided that information to the Australian government, and they denied that individual asylum, as they were contemplating.

Second, in November of last year, we assisted in a case of a Turkish man who was attempting to gain employment at a nuclear power plant. We were able to identify that he was using a false document with a false identity in an attempt to demonstrate his legal status in this country. He was obviously denied employment, but he was subsequently arrested for overstay and placed in Federal custody.

The third, which is not so distant from what you just reported, Senator Lieberman, was in October 2009, when the Canadians asked us to help them look at a boatload of undocumented males who were arriving off the coast of British Columbia. We helped them go through that with biometric information that they collected and identifying two of the individuals on that not only as suspected LTTE, Tamil Tiger terrorists, but also individuals who had sought visa and asylum status with us and were denied. Obviously, those individuals were detained.

So I think that represents the kind of thing that biometrics allow us to do, as you have so fervently supported on a number of occasions.

With respect to the role of the Coordinator for Counterterrorism, what has happened within the Department is, following the December 25, 2009, failed attempt to bomb Northwest Flight 253, the Secretary assigned me an additional responsibility for coordinating counterterrorism activities from the Department across its directorates, components, and offices related to detection, prevention, response to, and recovery from acts of terrorism.

In November of last year, she authorized the stand-up of a Counterterrorism Advisory Board to further improve coordination with the Coordinator acting as the Chair and the Under Secretary of Intelligence and Analysis and the Assistant Secretary for Policy to my left to act as the Vice Chairs. We have also organized under that a task force working group that supports this effort, so that what we are basically doing with respect to support for our mission one counterterrorism activity is use the Coordinator position, the Counterterrorism Advisory Board, and the task force to bring together intelligence, operational matters, policymaking elements

within the headquarters and the components so that we can field a cohesive and coordinated operational response to any threats that should arise or in some cases try to anticipate those threats.

Let me just give you one example of the kind of work that we have done. Following the death of Osama bin Laden, we began an even more dedicated review of intelligence. The CTAB was meeting on an almost daily basis for several weeks after that. We still meet roughly twice a week to look at these things. In each meeting, we look at new threat information. So in one case, we were looking at one particular threat and instituted a series of new measures that were put in place, taking the information that our intelligence and analysis office gave us, developing the countermeasures, creating the outreach to the various sectors who were affected by that particular piece of information, implementing those counterterrorism matters, informing State and local governments as well as other partners in our efforts, and basically coming up with a major effort to counter this particular threat. In addition to that, there was obviously a public affairs component.

This represents a much more coordinated response on the part of the Department than we have heretofore been able to produce and I think demonstrates the value.

In this particular case, we also considered whether we ought to raise the threat level and decided that the information was not sufficiently imminent and actionable so we chose not to do that. But that has nothing to do with the fact that we instituted security measures and had a public outreach program to ensure that we were adequately positioned, without having to raise the alert level, to respond to this particular threat.

In conclusion, we are working hard to address these complex challenges, and I stand ready to answer the questions from this Committee. Thank you very much.

Chairman LIEBERMAN. Thanks, Under Secretary Beers. That was a good beginning for us and a good report.

Next we are going to have Janice Jacobs, who is the Assistant Secretary, Bureau of Consular Affairs at the Department of State. Welcome back.

TESTIMONY OF HON. JANICE L. JACOBS,[1] ASSISTANT SECRETARY, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE

Ms. JACOBS. Thank you and good morning, Mr. Chairman and Senator Collins. It is an honor to appear before you again to tell you how the Department of State has increased security of the visa process in response to the December, 25, 2009, attempted terrorist act. In my previous appearances before this Committee, I testified about the Department's multilayered approach to visa security, what I had called "the five pillars of visa security": Technological advances, biometric innovations, personal interviews, data sharing, and training. I want to assure you that these pillars are even more relevant today. Today, after a full year of implementing corrective actions taken after December 25, 2009, I believe that our visa processing has reached new levels of security.

[1] The prepared statement of Ms. Jacobs appears in the Appendix on page 506.

The title of this hearing has a special meaning for the men and women of the Department of State. We have no higher priority than the safety of our fellow citizens and the protection of our borders. In this statement I would like briefly to highlight key steps we took to respond to the President's directive to address weaknesses in the systems and procedures we use to protect the United States.

We improved our Visas Viper Program and related processes by directing all chiefs of mission to ensure that the Visas Viper Program was working effectively at their posts and instructing consular officers to include complete information about all U.S. visas in Viper cables.

We issued new instructions to officers on visa revocation procedures and reinforced standing guidance on their discretionary authority to deny visas under Section 214(b) of the Immigration and Nationality Act, with specific reference to cases that raise security and other serious concerns.

We constantly refine and update the technology that supports our visa process. Before any visa is issued, the applicants fingerprints are screened against DHS's automatic biometric identification system called IDENT and against the FBI's Integrated Automated Fingerprint Identification System.

We use facial recognition technology to screen visa applicants against a watchlist of photos obtained from the Terrorist Screening Center as well as visa applicant photos contained in the Consolidated Consular Database.

We improved the capability of consular systems to match visa records against new and emerging derogatory information to support visa revocation in appropriate cases.

We employ sophisticated name-searching algorithms to ensure matches to derogatory information contained in the 39 million records pertaining to 27 million individuals found in the Consular Lookout and Support System. This layered biometric and biographic identity verification ensures the security of the U.S. visa by nearly eliminating the possibility of visa fraud through counterfeit or photo-substituted visas or through the use of valid visas by impostors.

We are continuing to match new threat information against our visa records. We have revoked over 1,000 visas since December 2009. As soon as a visa is revoked, a VRVK entry code is added to CLASS and shared in near real time with the DHS lookout systems used for border screening. CBP uses these VRVK records to advise airlines that certain passengers should not be boarded on flights bound for the United States.

We have completed the worldwide rollout of the online DS–160 non-immigrant visa application form, and we are currently piloting the online DS–260 immigrant visa application form. These forms provide consular and fraud prevention officers as well as our intelligence and law enforcement partners the opportunity to analyze data in advance of the visa interview.

Consular officers are trained to take all necessary steps to protect the United States and its citizens during the course of making visa decisions. Each consular officer completes our basic consular course, which has a strong emphasis on border security and fraud

prevention, and includes in-depth interviewing and name-checking technique training. Officers receive continuing education in all of these disciplines throughout their careers.

Consular officers receive extensive training on the Security Advisory Opinion process, which requires them to suspend visa processing pending interagency review of any case with possible terrorism ineligibilities. We work closely with DHS to ensure that no known terrorist receives a visa or is admitted into our country.

ICE special agents assigned to Visa Security Units provide timely and on-site vetting of visa applications and other law enforcement support to our consular officers. Over the past 7 years, the Department and DHS have increased resources significantly, improved procedures, and upgraded systems devoted to supporting the visa function.

DHS receives all of the information collected by the Department during the visa process and has broad access to our entire visa database. We make our visa information available to other agencies and specifically designed our systems to facilitate comprehensive data sharing. In May 2011, almost 22,000 officers from the Departments of Defense, Homeland Security, Justice, and Commerce submitted nearly 2 million visa record queries.

On a regular basis, we engage our foreign partners bilaterally, regionally, and on a multilateral basis to address the issue of terrorist travel. We have entered into arrangements for the sharing of visa information with foreign governments consistent with the data protection requirements of Section 222(f) of the INA.

With our partners at the Terrorist Screening Center, we negotiate Homeland Security Presidential Directive 6 agreements overseas. We are a close partner with DHS in advance passenger information and passenger name record discussions overseas.

Anne Witkowsky, our Deputy Coordinator for Homeland Security and Multilateral Affairs in the Office of the Coordinator for Counterterrorism, is here with me today to answer any questions you may have on building foreign partner antiterrorism capacity or the State Department's role in the overall U.S. Government terrorist travel strategy.

Let me also address the Committee's interest in the process that brings Iraqi nationals working on behalf of the U.S. Government in Iraq to this country as recipients of special immigrant visas or as refugees.

As of mid-June a total of 7,063 Iraqis have been issued special immigrant visas under one of the two pertinent SIV programs. Kelly Gauger of the Refugee Affairs Office within the Bureau of Population, Refugees, and Migration is here to answer questions about the State Department's role in U.S. refugee security screening.

Distinguished Members of the Committee, I believe that a layered approach to border security screening in which each agency applies its particular strengths and expertise best serves our border security agenda while furthering traditional U.S. interests in legitimate travel, trade promotion, and the exchange of ideas. The United States must meet both goals to guarantee our long-term security.

Thank you and I am ready to answer your questions.

Chairman LIEBERMAN. Thanks, Assistant Secretary Jacobs.

The Senate is in a quorum call, which means that hopefully we can hear the opening statement of David Heyman, who is the Assistant Secretary in charge of the Office of Policy at DHS. Thank you.

TESTIMONY OF HON. DAVID F. HEYMAN,[1] ASSISTANT SECRETARY, OFFICE OF POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HEYMAN. Mr. Chairman, Senator Collins, and Senator Paul, this hearing, preventing terrorists from traveling to or remaining undetected in the United States, remains a top priority at the Department.

Ten years ago, screening of passengers coming to the United States was limited to the Department of State visa process, if applicable, and the inspection of a person by an immigration officer at the port of entry, plus whatever processes were applied at foreign airports or by foreign governments. If you were a terrorist seeking to come to the United States, you would, for all intents and purposes, apply for a visa, purchase a ticket, and board an aircraft to America. There would be very limited checks to see if you were known or suspected of terrorist activities other than the visa process, limited checks to see if you may be a security risk based upon your behavior, no checks to see if you were traveling under a lost or stolen passport, limited checks on you or your baggage for explosives, and little to no security on board the aircraft during the flight, as well as limited checks to see even if you are admissible to the United States. That was 10 years ago.

Similarly, at that time provision of advance passenger information was voluntary, and even when provided by air carriers, it frequently contained inaccurate or incomplete information. There was no biometric collection for visa applicants beyond photographs nor for aliens seeking admission to the United States, and there was very limited pre-departure screening of passengers seeking to fly to the United States.

Today, a decade later, in response to both 9/11 and evolving threats, and with the help and support of this Congress, we have significantly adapted and enhanced our ability to detect and interdict travel threats at the earliest opportunity. The systems we have put in place over the past decade are multilayered and multinational, from the intelligence we gather on known and suspected terrorists even before someone decides to travel to the United States to visa and travel authorization processes, travel document security, pre-flight screening against criminal and terrorist databases, checkpoint screening prior to boarding, pre-departure screening for admissibility to the United States, in-flight security, and additional screening at ports of entry. We have put in place multiple layers of security across the spectrum of travel—before departure, during travel, and upon arrival.

Additionally, we have put in place or are in the process of piloting recurrent vetting programs to check and recheck the status and potential risks of all visa holders and immigrants after they arrive

[1] The prepared statement of Mr. Heyman appears in the Appendix on page 530.

into the United States. Today, all air and sea passengers intending to travel to the United States must have valid visas or, if traveling under the Visa Waiver Program, must now obtain in advance of travel electronic travel authorization.

Since 2009, under the Western Hemisphere Travel Initiative and in support of key 9/11 Commission recommendations, all travelers coming across our land borders are required to establish identity and citizenship. Furthermore, while issuing visas is the responsibility of the Department of State, as you have mentioned, at certain embassies and consulates DHS administers a Visa Security Program through ICE where we assist the State Department in identifying visa applicants who may present a security threat.

Prior to 9/11, there was no centralized system or method to screen airline passengers. Over the past 10 years, the U.S. Government has stood up the Terrorist Screening Center administered by the FBI and established a consolidated terrorist screening database or watchlist to determine who may be authorized to travel to the United States, who may board a plane, and who may require further screening.

Additionally, fulfilling another key 9/11 Commission recommendation, DHS and the TSA have strengthened security through full implementation of the Secure Flight Program. Under the Secure Flight Program, DHS now pre-screens 100 percent of passengers on flights flying to, from, or within the United States against the no-fly and selectee portions of the known and suspected terrorist watchlist. Through the Secure Flight Program, TSA now vets over 2 million passengers daily.

We have expanded our trusted traveler programs from approximately 80,000 members when DHS was created to well over a million people today, and by expanding these programs, these passengers, who provide biometric identification and pass rigorous recurrent security checks, we are now better able to focus resources and attention on those who may pose a greater risk.

DHS also uses passenger name record data which is the information that travelers provide airlines when they book a flight. This information, along with the APIS and the Immigration Advisory Program, allows us to assess a passenger's level of risk prior to departure, and when necessary, flag them for further inspection or even prevent them from boarding.

Following the attempted attack of December 25, 2009, DHS implemented additional enhancements in coordination with other departments. These include a number of items which I have complete in my testimony, but let me just list a couple now.

The U.S. Government reformed the criteria and nomination processes for the terrorist watchlist and enhanced its information-sharing capabilities.

We updated the Secure Flight Program to use all terrorist watchlist records containing a full name and a full date of birth. Travelers are then required for enhanced physical screening prior to boarding.

Beginning in 2010, DHS began a new initiative with the Department of State where CBP currently vets approved visa applications so that as new information is discovered, DHS and the Department

of State are able to proactively identify these individuals and address them.

Also, beginning earlier this year, DHS began piloting a new recurrent vetting process for those applying for immigration benefits. As new derogatory information surfaces, we double-check those who have approved immigration status against this information.

In addition, prior to December 25, 2009, CBP conducted inbound passenger targeting using APIS and PNR data provided by the airlines but could not easily prevent high-risk travelers from boarding flights to the United States unless they were traveling from foreign locations where we had our Immigration Advisory Program or preclearance presence. As of December 25, CBP re-engineered its inbound targeting operations to identify high-risk travelers who are likely to be inadmissible and recommend to carriers at all airports, all last points of departures, that those individuals not be permitted to board a commercial aircraft.

DHS has also strengthened the presence and capacity of law enforcement to prevent terrorist attacks on aviation to include our Federal air marshals and FAMS coverage.

And, finally, I think the lesson of Abdulmutallab, or one of them, is that if you have access to one airport anywhere in the world, you have access to the entire international aviation system, and so to prevent terrorist travel, we must work closely with our international partners. We did just that following December 25, 2012. In the weeks and months that followed that event, DHS worked with the International Civil Aviation Organization, and on a bilateral basis, to advance an unprecedented initiative and to strengthen aviation security. Those efforts culminated at the ICAO Triennial Assembly in October 2010 where the assembly adopted the Declaration on Aviation Security, which forges a new foundation for aviation security to better protect the entire global aviation system. The extraordinary global collaboration demonstrated by nearly 190 countries during that assembly has helped to bring about an aviation security framework that will help make air travel safer and more secure.

All of this is not to say that there will not be new threats or that the security architecture is a finished product. To the contrary, this effort will require continuous improvement. Terrorist screening is a multiagency effort that relies on good data, good intelligence and information, automated capabilities to ensure identification of high-risk activities and individuals. We must continue to understand the threat, terrorist tactics, and stay ahead of it. This requires strong interagency and international partnerships, something that we are deeply committed to.

As a result of all of these efforts over the last decade, it is now part of our regular daily experience to identify potential incoming threats and deny them boarding, deny them admission, and at a minimum require them to go through enhanced screening. CBP through its National Targeting Center generates nearly 200 targets a day of where they have to research whether they should be boarded or not. They have identified 2,600 passengers that would likely have been found inadmissible upon arrival and passed that on to air carriers.

TSA now vets over 14 million passengers weekly; approximately 25 individuals per month are denied boarding on aircraft through the Secure Flight Program.

Let me conclude by saying that this Nation I think has taken significant steps to counter and prevent terrorist travel since 9/11. This has been accomplished as a result of a historic partnership between Federal agencies, between Federal, State, and local partners, between multiple Congresses, and three successive Administrations, and with our international partners. It entails a multilayered, multifaceted, and multinational effort that weaves together intelligence, information sharing, security and law enforcement programs from across DHS, the interagency, and across multiple partners around the world. Together they reflect one of the Nation's most pressing priorities: To ensure the safe, secure, and efficient movement of literally millions of people traveling to, from, and around the United States on a daily basis, while thwarting the few would-be terrorists to who seek to do us harm.

This concludes my testimony. I have a written statement for the record, and I look forward to your questions. Thank you.

Chairman LIEBERMAN. Thanks, Assistant Secretary Heyman. Your statement and that of the other witnesses will be included in full in the record.

I appreciate your testimony. It was actually quite revealing to hear the description before and after 9/11 of what you have to go through to get into the country. We know in this Committee pretty well what has happened since 9/11, but it was important to be reminded about how easy it was to get into the United States prior to 9/11 if you intended to do us harm. And I think hearing all we have done since then ought to give people in our country some increased sense of security when they go about their daily lives but also, of course, when they travel. But obviously we are never going to achieve everything we want by way of security and also retain the freedom of movement that is part of what defines us as Americans. So when we come back, I am sure we will be asking the three of you about some things that we think should be done better.

Let us close on this good note and thank you for all you have done to bring us to the point we are at. I am glad we could get the three of you in. We will come back as soon as we can from the two votes.

The hearing is in recess.

[Recess.]

Chairman LIEBERMAN. The hearing will come back to order. Thank you very much for your patience while we were voting. We will do 7-minute rounds of questions.

Let me begin with a question for you, Assistant Secretary Jacobs. A recent GAO report, which was a review of the Visa Security Program, raised some questions about how it was working. One of the most troubling parts of the report to me was that GAO found disagreements between consular officers and Immigration and Custom Enforcement agents, at some posts around the world concerning how close an association with terrorism was needed before someone could be denied a visa to come into the United States. I would guess that most Americans would share the opinion I have, which is that travel to the United States is a privilege not a right and

that any association with terrorism should be enough to keep a foreign national from getting a visa to come into the United States.

So I wanted to ask you to respond to that finding by the GAO and tell the Committee exactly what the policy of the State Department is now. What kind of association with terrorism would be considered significant enough to bar someone from being issued a visa? And then, Mr. Beers or Mr. Heyman, if you have anything to add from the perspective of DHS, being the Department in which ICE is located, I would welcome that testimony as well. Ms. Jacobs.

Ms. JACOBS. Thank you, Senator. Basically let me start off by saying that I think that we have very good cooperation between the VSUs and the consular sections, wherever the Visa Security Program is in place. And it is true from time to time that looking at the exact same information, two individuals might come to different conclusions.

We have found, though, in every single case—first of all, those are few and far between. In most every instance there is agreement. But when there is a disagreement, normally it is worked out at post where people will sit down and really look at the information and try to decide whether, in fact, it makes someone either ineligible for a visa or inadmissible to the United States.

If for some reason they cannot reach agreement there, then the case is referred back to headquarters where people in Consular Affairs and people at DHS will take a look at it. And then it is always resolved there.

When we signed the MOU with DHS back in 2003 on our shared roles and responsibilities on visas, we actually put in place there a very formal mechanism if there was a dispute or a disagreement that could not be resolved at those levels where the Secretaries would get involved, and then we would resolve it that way. That has never happened. It has never had to happen. As I said, most of these are taken care of right at post.

Chairman LIEBERMAN. So what is the State Department policy now on this question? And do the disputes go to the weight of the evidence when there are disputes? I understand you have said that the disputes between State and Homeland Security are rare, but is there a State Department policy?

Ms. JACOBS. The policy really is simply to apply the existing provisions of law, and so if there is information suggesting that someone might have some kind of connection to terrorism, the ICE officer might look at it and come to one conclusion, whereas the consular officer may look at it and believe that it is not sufficient to find the person ineligible for a visa. But in any case, we will always give security the priority when we are adjudicating visas, and if there is any question or doubt, the burden of proof is on the applicant.

Chairman LIEBERMAN. Good.

Ms. JACOBS. The law is written in a way that puts the burden of proof on the applicant.

Chairman LIEBERMAN. That is important.

Ms. JACOBS. And so we would in almost all instances wind up denying the visa.

Chairman LIEBERMAN. Do you have anything you want to add to that, Mr. Beers or Mr. Heyman? It is not necessary.

Mr. BEERS. No, sir. I think that is a fair rendition of our ability to cooperate with one another.

Chairman LIEBERMAN. Good. Let me go in the time I have remaining in this round to this question of the US-VISIT exit system. This is a source of concern. I know it is no small task, but this is not only a question that leads to an enormous number of so-called illegal immigrants who do not come in illegally but then stay here illegally, but also in some cases obviously related to terrorist activity. My recollection is that three of the 9/11 terrorists were here because they had overstayed legal visas, and, of course, if you think about it, it is one of the remaining ways somebody who has a nefarious intent to come in as a tourist or a student and then overstay and attack the United States.

So this backlog of 1.6 million people, give us your report on why we are behind on that and what we are doing now to catch up.

Mr. BEERS. Thank you, sir, for the opportunity to answer this question because we have been working hard on dealing with that issue over the last several weeks, and I think I am in a position to say that we will have cleared the backlog later this week or early next week. But let me tell you what we have done——

Chairman LIEBERMAN. That is significant.

Mr. BEERS. So that you actually understand what we have done.

Chairman LIEBERMAN. Yes.

Mr. BEERS. We have taken the 1.6 million, and we have run it against two databases: One which said, Did this individual leave the United States after they went into an overstay status? Or did this individual change to a different visa or a different benefit? And we have basically eliminated 50 percent of the people in the 1.6 million.

Chairman LIEBERMAN. Just so I understand, that is very interesting it is that high a percentage. So they either left——

Mr. BEERS. But in an overstay status.

Chairman LIEBERMAN. Right. So we had some record of that. And then second is that they had changed their status?

Mr. BEERS. They applied for a different visa, or they came in and applied for a different benefit status.

Chairman LIEBERMAN. Yes, and in the current state of recordkeeping we did not know that.

Mr. BEERS. What we had not done is when they went into overstay status, if they were not in the priority category that we were looking at before we ran this broad check, we did not look at them. And what we decided we had to do in response both to our own concerns and your concerns is we needed to get through all of them.

So what we have done is those people have left—those who were in an overstay status and left will be caught if they try to come in again, because having been in an overstay status, that is a basis for denying them a visa or a basis of refusing entry to a visa waiver person who seeks to come in again.

With respect to the remaining 50 percent, what we are doing at this point in time is running them against CBP's travel history to see whether or not they would have hit any of our targeting rules

and been the basis for having an additional interrogation. In some cases, sir, this is information that came in after they entered the United States.

The second thing we are doing is we are sharing the database with the intelligence community through NCTC to see if there is any additional derogatory information. As we are able to transfer this information to ICE, we can allow ICE to be able to look at not just the original way in which we had sorted the data, but across all of the people who have come into the United States or are in an overstay status so that they can then prioritize those particular individuals that they want to go after in the first instance.

Obviously, we do not want anybody to overstay in this country, and as you well know, we have limited resources, and ICE will, therefore, prioritize who they are going after. But this will give us a much better picture.

When we have finished with this process, sir, we want to come up and brief the Committee on the results of this. So I am telling you is what the process looks like. What I want to come back to tell you or have staff come back and tell you is what that process yielded: What did we learn? What are we doing about it? And how will we do this better?

Chairman LIEBERMAN. I am interested in this—and I think it is significant. I would like to ask you to come back and brief Senator Collins and me and anybody else on the Committee who wants to be there. Do you have a sense of how soon you will be ready to do that?

Mr. BEERS. Sir, I am expecting to review the data either later this week or early next week. As soon as I have heard the report, we will put things together and get back to you. I do not want to promise next week.

Chairman LIEBERMAN. No, that is fine. That gives us a general sense.

Mr. BEERS. Let me say we will get back to you before the August recess, sir.

Chairman LIEBERMAN. Fine. My time is really over, so maybe I will come back to this. Now that you have worked to try to clear up the backlog, how do we get to the end state we want to get to, including particularly a comprehensive, functioning biometric exit system? But in deference to my colleagues, I am going to hold that one and call on Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I want to leave the majority of the questions about the Kentucky case to my colleague from Kentucky, but I do want to ask one general overview question. Assistant Secretary Jacobs, it is my understanding that since 2007, the U.S. Refugee Admissions Program, which was the program under which these two alleged terrorists were settled in Kentucky, has approved more than 84,000 Iraqi nationals for resettlement, and 58,810 Iraqi refugees have actually arrived in the United States.

What is being done to ensure that there are not other cases like those two alleged terrorists in Kentucky among those 58,000 that are already here in addition to the 30,000 additional ones that have been approved for resettlement?

Ms. JACOBS. Thank you, Senator. For the Refugee Admissions Program, actually we have shared responsibilities with the Department of Homeland Security, and the State Department does play a role before people arrive in the United States, and then once they are here, they are under the purview of the Department of Homeland Security.

I can tell you just generally that over the past few months we have put in place more stringent screening requirements for both refugees and for special immigrant visa applicants who want to come to the United States, and we can probably give you more details about exactly what that screening consists of in a classified briefing. But please know that has happened and certainly anyone who is currently outside of the United States wanting to come here is undergoing that new level of scrutiny.

I don't know if one of my DHS colleagues wants to talk about the actual screening of people once they have arrived here.

Senator COLLINS. Well, I am concerned about people being approved to come, but I am concerned about the 58,000 already here. Is there a review being done of those who are here to make sure that there are not other cases of individuals who should not have been admitted? Assistant Secretary Heyman.

Mr. HEYMAN. Yes. The answer to your question is yes, Senator. Several months ago we began a pilot project to enhance our screening both abroad before individuals come here as part of the Refugee and Asylee Program, but also looking retrospectively. The Iraqi program in particular started back in 2007, and so we have had vetting in place since then to include looking at holdings from other agencies. And so what we are doing now is to look again in a recurrent fashion or in an enhanced re-check fashion, and we are piloting that effort right now to see the technical capability of doing that and also what we are finding. That will be concluded at the end of this month, and we can get back to you and let you know what results we found.

Senator COLLINS. The Chairman and I are working on a DHS reauthorization bill, as Assistant Secretary Beers knows because he is smiling as I say that. Whether in approval or in horror, I am not sure. But when I was reading the most recent GAO report that I requested, which was released today, GAO found a lot of redundancies, examples of travel offices at the Department of State being unaware of training programs at the Department of Homeland Security. And it seems as though there are several offices that are involved in terrorist travel: The US–VISIT program, the Screening Coordination Office, and the Visa Waiver Program.

I have concerns based on GAO's findings about duplication, a lack of communication, and coordination. As we are looking at the reauthorization bill, I would like all of you to comment on whether there should be a single office that deals with terrorist travel and all of these programs, with the exception of TSA, which is clearly a different kind of screening program. Assistant Secretary Beers.

Mr. BEERS. Let me start. We have TSA, we have CBP, we have USCIS, all of whom are front-line activities that deal directly with terrorist travel, and we have ICE on top of that, which has an enforcement function.

What we have tried to do with respect to this kind of an issue is exactly why the position of the Coordinator for Counterterrorism was established, to try to ask the question that you are asking and ensure in short order that the deficiencies that might be occurring in fact are corrected and that we have this kind of coordination.

With respect to the issue that you asked and with respect to the GAO report, Assistant Secretary Jacobs and I have also talked about the coordination that needs to happen between our Department and her Department. Now, obviously, some of that should have happened in the embassy when the country team was aware that there were two different agencies coming in roughly the same time frame to talk to the same people. That should not happen. There is no question about that.

So we have certainly agreed that we are going to do a better job across agencies to do that, but we have to do the same thing within the Department on training.

The Secretary has asked us specifically to look at these kinds of overseas positions and overseas travel, so Assistant Secretary Heyman, who is responsible for the Office of International Affairs, also has a very important role to play in that, and he may want to add something on that.

Senator COLLINS. Assistant Secretary Heyman, should there be a consolidation of some of these programs within one office?

Mr. HEYMAN. So, Under Secretary Beers rightly points out that almost every part of the Department has some role to play in screening or addressing travel screening as it pertains to individuals coming into this country. I would add also the U.S. Coast Guard in the maritime domain as well. And so that is why we established the Screening Coordination Office from a policy perspective to make sure that from a policy perspective we have the right framework and coordination across the Department.

The role of the Coordinator for Counterterrorism is to make sure operationally that these entities are all working together and there is no duplication or that there are no gaps. And so I think the combination of a Screening Coordination Office to make sure that our policies across the Department are uniform, consistent, and appropriate and a Counterterrorism Coordinator looking at the symphony of these parts moving is being conducted in a harmonious way, if I get the metaphor right, I think that is an approach that I think is quite useful. We have seen it effective in the short time that the process has been operational.

Senator COLLINS. Assistant Secretary Jacobs, if you could quickly comment since obviously we have heard how DHS is coordinating with the Department, but the fact is the State Department plays a considerable role.

Ms. JACOBS. Yes, Senator, that is right. We do. We have our Office of Counterterrorism where we have a number of regional and other programs that they oversee. Some of that is capacity building, some of it is training.

I think the areas where we sometimes run into duplication, because we have similar missions, is on fraud training, and that particular example pointed out in the GAO report, as Under Secretary Beers pointed out, really should not have happened because it is

incumbent upon the country team at a post to know who is coming in and to prevent that kind of duplication from taking place.

I think that within the U.S. Government as a whole, again, our Office of the Coordinator for Counterterrorism plays a significant role in the overseas programs. I think that we can probably do a better job working with our DHS colleagues in the specific areas where we seem to have similar missions such as, again, fighting fraud, helping foreign officials identify fraudulent documents. We have expertise, both of us, in that area, and perhaps we can even go together and do this kind of training, which would be even more effective. So I am certainly willing to sit down and talk to my DHS colleagues about how we might do a better job with that.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Paul.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Thank you, Mr. Chairman and Senator Collins, for putting these hearings together, and I thank the panel for coming.

I think the most serious threats to our country from terrorism probably come from travel visas, refugee visas, and student visas. Now, some might argue with that, but 16 of the 19 hijackers were here on student visas, were not policed well, and had overstayed their welcome. I am still concerned we may not have figured out nor done a good enough job on these problems.

I believe we continue to have security breaches, and I think there are two possibilities. We could say, well, there are so many people visiting that we will have these breaches; it is inevitable we will have a certain amount. Or you could say that maybe we are inundated with information and it is our philosophy that is mistaken.

Perhaps it is that our philosophy is that everyone is potentially a terrorist and everyone has an equal chance of being a terrorist. I think if you take that philosophy, you inundate yourself with information, so much information that you will never get through it. Nobody can talk to each other because you are wallowing in electronic and paper information, and you cannot determine who the people are, which would really require good police work.

We had the head of the TSA here last week. After we showed him the outrage—and he has to be reading the newspaper—over patting down these children, he said TSA was changing its procedure. But then he sends me a rather curt note and says, "well, an 8-year-old had a bomb in Afghanistan."

The problem is there is a logical error there—an 8-year-old in Afghanistan had a bomb. What does that have to do with an 8-year-old or a 6-year-old in Bowling Green? Absolutely nothing. Now, they are the same age, but that is not a risk factor, and age is not a risk factor. It is where this girl lived, how she grew up. It is sort of like telling me that if an 8-year-old in Afghanistan sacrifices a goat, we now have to be worried about kids sacrificing goats at 8 in America. They have nothing to do with each other, but that is the logic. But it is this universal approach that everyone is the same and everyone is an equal threat. But I think it makes us less safe, but it makes us more insulted.

This morning, in the airport in Nashville, a 41-year-old mother was arrested because she did not want TSA agents putting their hands inside the pants of her 6-year-old girl. They say they are going to change, but they are not changing. They continue to pat down 6-year-old girls. The real threat is from people who are coming here internationally.

So here we get to the situation in Bowling Green. I compliment the FBI and our local law enforcement for doing a good job, but I think this person was only caught because an informant tipped them off, and then we finally started looking, and eventually we looked through a database that we had not been looking through.

Chairman Lieberman remarks that this is from the FBI database. Why wasn't this going on? Why does it take an informant to find somebody for us for us to do our job? Do we need to replace people who are not doing their job? It sounds like no one thought this through since we had to be tipped off by an informant, and then we are left saying: "Oh, my goodness, we let a terrorist in."

But it gets back to the universal versus the specific. Why can't we search everybody? Why don't we know everybody's background? Because we have let 60,000 Iraqis in here in the last 3 years. It is a policy question. Why do you admit 60,000 people?

Now, here is the point: People will argue, well, it is dangerous over there. Well, we have 50,000 of our young men and women putting their lives on the line every day. Some of our relatives, some of my relatives, are over there putting their lives on the line for the Iraqis. Do you think maybe they ought to stay even if it is a dangerous place? It has been dangerous since the 900 A.D. Karbala massacre—not the recent massacre. They have hated each other for a millennium. It is not safe. But should we be admitting 50,000 people over here to our country?

And then to add insult to injury, one of the alleged attackers who lived in government housing—most of them do. We are encouraging them to be on welfare. We have a whole cottage industry set up to get them in government housing, and on food stamps. It is insulting to us that we are doing this, but it would take a policy change. I do not fault you for missing the needle in the haystack. You have to make the haystack smaller. We need to admit fewer people. There is no reason we should be admitting 60,000 people, and we need to address that policy.

I am almost out of breath. Why don't we start with that question, Mr. Heyman, and tell me: Why do we need 60,000? Are we going to keep admitting 18,000 a year? Can we possibly know who these people are?

And just one other example of how we cannot. Even in the military over there—we have an attack almost every 6 months where we admit someone into the Iraqi military or the Afghan military, and then they attack our soldiers on base. It is hard to know who your friends are and who your foes are because they will lie to you on the admission statement.

But I would appreciate your comments, Assistant Secretary Heyman.

Mr. HEYMAN. Thank you, Senator, and I might add this is the first hearing I have been at where there are two individuals with

the first name of Rand, and I am not sure I will ever experience that again. [Laughter.]

Senator, the decision, I think, after the war in Iraq to admit Iraqis who had helped United States and coalition forces in that endeavor, whether as interpreters, informants, or otherwise, was a decision that was taken back in, I think, 2006 or 2007. It continues to be the policy of this government that those individuals who also may be at risk of retribution or those individuals who supported the United States in such ways, they and their families would be given an opportunity to come here.

Senator PAUL. Let me interject. Here is the difference, though. In Vietnam, the war ended and a totalitarian regime took over, and I have many friends who came here from South Vietnam who fought with us. I do not have any problem with that. We should reward people who fought with us, we fought with them. But it is not a totalitarian regime. We have a democracy over there. We are supposed to be proud of that government. It is not perfectly safe over there, but there is no reason to continue this policy, and the policy should change.

Mr. HEYMAN. Let me get also to the really, I think, strong point you made about a universal policy of terrorists behind every person versus a possibility of using more discriminating tactics and approach, which is what we attempt to do. We have adopted a risk-based approach to security. I believe John Pistole, the head of TSA, testified to some of the things we have been trying to do as recently as a month or so ago, which is to expand the list of those who are, in fact, trusted to us or known to us, the trusted travelers who do not require the kind of screening that those who might pose a threat to us do. And so in terms of moving forward with that, I know that Administrator Pistole has already brought in the pilots and pilots association into that trusted program——

Senator PAUL. But I do not think he is doing any less patdowns. He said he was going to change his policy on patdowns. Every day there are more complaints. It is insulting our privacy. Our parents do not like it. Our kids do not like it. It needs to change. Our approach should not be: Because there was an 8-year-old with a bomb in Afghanistan, all 8-year-olds in America are a threat to our country. It is not true, it is a waste of time, and you are not going after the people who could attack us. We have a guy who gets on a plane with 11 different boarding passes, he gets on with his student ID from Michigan and a boarding pass with the wrong name on it. TSA does not catch him, but they are insulting all of the little children in our country, and it needs to stop. They need to change the policy. They do not need to come here and tell us their policy is changing and continue to do the same thing, and that is what he told me in his letter. He is going to continue patting them down because he found an 8-year-old with a bomb in Afghanistan.

I know it is not all your fault, but I have to let off some steam.

Mr. HEYMAN. I appreciate that, and actually also just let me at least recognize that 2 million individuals go through TSA's screening every day. Our TSA front-line officials have to make those kinds of difficult judgments, not always successfully in the cases that you have brought forward, but they do process 2 million peo-

ple a day, and I think they do it at a very high professional rate. Thanks.

Senator PAUL. Can I have just a couple more minutes? I have a couple other questions.

The 59,000 refugees that Senator Collins brought up, you say you are going to screen them. Right now how many of the 59,000 have been re-screened? And will every individual, all 59,000, be re-screened?

Mr. HEYMAN. I do not have the numbers. I can get back to you on the specifics of that.

Mr. BEERS. The number we will re-screen is all of them.

Senator PAUL. You will screen all 59,000.

Mr. BEERS. All have been re-screened at least once. This is not going to be a one-time-only screening process because, as you are well aware, information becomes available, even if it is historical, that does not become available until a time later. So this is a program that we have instituted which is both backward-looking and forward-looking. We have been through the backlog. It is a large number, as you quite correctly said, and it was not an easy process because it required some database adjustments and interactions that we had not even tried before.

So I can tell you, as a result of that, we have had some important new insights into how we need to have our databases fit together and be integrated with one another.

Senator PAUL. With the student visa program, we admit 40,000 people from the Middle East, 20,000 from Saudi Arabia; 16 of the 19 hijackers were from Saudi Arabia; 16 of the 19 I think were also overstaying their student visas.

Are the student visa people initially going through the better process now that would hopefully catch people who have fingerprints in there? Are they going through the same kind of screening before they come here?

Mr. HEYMAN. All of our visa applicants go through a number of screening processes that I described, including matches against the known or suspected terrorist watchlist, targeting against unknown behavioral patterns, criminal databases, as well as additional visa violations.

Senator PAUL. And supposedly the better screening, not the screening we did 2 years ago that did not work, we now have enhanced, and they are doing——

Mr. HEYMAN. We have had extensive improvements in screening and in our watchlisting process as recently as in the past 2 years, but also over the last several years.

Senator PAUL. Are they re-screened again? If they enroll in school, do we know they are still in school after 3 months? Does someone go through all 40,000 and find out if they are attending classes? Not enrolled. Attending classes.

Ms. JACOBS. All of the foreign students who come here participate in the SEVIS program, which is basically a program that monitors their attendance at school when they first enroll. Any switch in schools is registered in that system. Consular officers overseas have access to that system, and let me just add that before they even get their student visa, as a visa applicant they go through a number of security checks, including being run through our lookout

system, which has about 39 million records, 70 percent of which come from other agencies, many of those law enforcement and intelligence agencies. So there is a thorough screening before they come, and once they get here they have to maintain status. If they are not registered in this system that I described, SEVIS, then their names are turned over to ICE.

Senator PAUL. So attendance is being recorded by whom? By the school and then sent back? That is how the system works?

Ms. JACOBS. The school, yes, has the responsibility for——

Senator PAUL. If they overstay their welcome, if they overstay their student visa, are we systematically going through—like Senator Lieberman talked about with the exit program, do we have an exit program on all student visas?

Mr. BEERS. It is one of all of the visas that we look at, yes. If they go into overstay status, it is noted, and now we have this vetting system that will focus on anybody who is an overstay to ensure that we know as much as possible about it.

What we will end up having to do now is, as this number of unreviewed overstays goes to zero, we will then have to continue to do recurrent vetting to make sure that the individuals who were placed in an overstay status, who then leave after we have reviewed their files initially, we come back and make sure that we know that they have actually left the country so that we can inform ICE that is not a person who is an overstay status.

Senator PAUL. And one quick final question on the Bowling Green alleged terrorists. If their fingerprints were in an FBI database, why weren't they checked?

Mr. BEERS. We did not have access to that database, sir.

Senator PAUL. I am not sure I understand that.

Mr. BEERS. We get a lot of fingerprints from a lot of different sources, including the FBI. We did not have access to that fingerprint in the US–VISIT system, which is the way that we then are able to make the identification. That person, had that information been available, would have immediately come up on the FBI's radar screen independent of the informant coming forward.

Senator PAUL. That is a real problem. I mean, we got lucky because of the informant, but I guess that is the real problem, and I do not understand. See, I do not know all the names of your watchlists, but I have heard of the FBI. I would think that would be a pretty prominent watchlist or database fingerprints where you would be integrating your information.

Mr. BEERS. Sir, you need to ask the FBI to explain where that particular fingerprint was.

Senator PAUL. I am going to ask them. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Paul. We will ask the FBI that. I gather they are far behind—but there is no excuse for that—on inputting fingerprints of this kind. But I do not understand why it would be 5 or 6 years.

No need to regret your agitation or letting off steam here. We share your agitation, and your right to let off steam is fully protected here in this Committee, and that right has been exploited by many Members of the Committee over time, one of which is our next distinguished colleague from Massachusetts. [Laughter.]

Senator Brown.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. Thank you, Mr. Chairman.

Assistant Secretary Jacobs, due to the recent political turmoil in Yemen, the State Department has withdrawn most of the staff from the embassy in Sana'a. However, before this occurred, earlier in the year, the OIG found that in 2009 and 2010 the embassy in Sana'a was, in fact, critically understaffed, and fraud prevention, as you know, is critical to preventing terrorists from getting visas to come to the United States, and probably one of the most important places that we need to ensure we have necessary resources to fulfill this critical function is in Yemen, especially now, where AQAP is actively plotting to conduct attacks on the United States. Yet according to the State Department's OIG, the embassy is in critical need of staffing, in the Fraud Prevention Unit, especially.

So how can we effectuate counterterrorism policies if the necessary resources are not being supplied?

Ms. JACOBS. Thank you, Senator. It is absolutely true that our embassy in Sana'a, in Yemen, traditionally has been a place where it has been hard to fill positions. It is a difficult place and sometimes difficult to get people to those positions that exist.

The State Department has made it a priority to make sure, though, that with these critical countries like Yemen we are getting not just the staffing filling a position, but filling the position with the right people, and that is a top priority for the State Department. The truth is we are on ordered departure right now in Sana'a, so a number of the people who were at the embassy have had to leave, but that does not mean that we in any way have cut back in our consular section on fraud prevention or really screening the applicants.

We understand very well the high risks that exist in Yemen and the fact that applicants there have to undergo very extensive scrutiny.

I have made it a personal quest, after visiting Sana'a almost 2 years ago, to make sure that the consular section in that embassy is not just properly staffed but has the right people in it. I have sent a number of my very best officers to temporarily head the consular section. We now have a permanent person who just arrived, someone who is one of our best officers, who is going to be running our operation there.

I have sent in a number of temporary officers to reduce backlogs, to look especially at fraud and what we are doing to prevent that.

We have help from our diplomatic security colleagues. We have an assistant RSO investigator who helps us with our fraud investigations in Sana'a. We have a Visa Security Unit there. A lot of different people with the very same concerns, with the same mission, and that is, to keep out people who might be coming here to do us harm.

Senator BROWN. But even though you are doing that, it is still understaffed.

Ms. JACOBS. The consular section is not understaffed.

Senator BROWN. It is not. How many people do you actually have working in that section?

Ms. JACOBS. I will get back to you with the exact number.

Senator BROWN. Yes, if you could, let me know how many people are working there, where the shortfall is, if any, and how many efforts do you process monthly because if there is a breakdown and there is something that we need to do to help get that up. I mean, it is no secret that Yemen is in the forefront of terrorist activity, and to think that we may be, because of lack of resources, allowing people to sneak through the cracks is problematic and very troubling. So I would rather be proactive, and then if there is something that the Chairman, in his amazing leadership, and Senator Collins can do to provide the resources to fill that void, that would be helpful.

Assistant Secretary Heyman, thank you, sir. Is it my understanding that there is a backlog of over—and this may have been asked, and I apologize. I actually just had a briefing on Yemen, so I was a little delayed. But is there a backlog of over 1.6 million potential visa overstays? I think that is what Mr. Beers was hinting at. Is that number accurate?

Mr. BEERS. Sir, that is my bailiwick.

Senator BROWN. Oh, I am sorry, sir.

Mr. BEERS. That is quite all right. There was a backlog of 1.6 million. Over the last several weeks, we have worked at a very high level of activity to deal with this.

Senator BROWN. So what is the number now, do you think?

Mr. BEERS. The number is less than half of that number in that the people who were included in that 1.6 million, over half of them have already left the country. They were in an overstay status when they left the country, but they left the country after they passed into the overstay status, and we had not determined that.

There is a much smaller number who have changed status; that is, they have applied for a different visa or in some cases they may have had an application for refugee status or something along those lines.

The remaining people—just to assure you, anybody who left after they were an overstay will not be admitted again because we have their biometric data, and if they apply for a visa, they will be denied a visa because they overstayed on an earlier visa. And if they come through the Visa Waiver Program, we have their biometric data in that way, and we will see who they are when they seek to get off the plane and pass through immigration. They will not be admitted. They will be returned to the country from which they came. So that is the first half.

Then the second half——

Senator BROWN. Let me just stay on that first half. Is it true that it is 180 days after their visa expires that they are considered having overstayed their visa?

Mr. BEERS. We know when they overstay on the day that they have overstayed.

Senator BROWN. Yes, but we are a non-visa waiver country and we do not consider them really overstayed until 180 days. Isn't that right?

Mr. BEERS. Well, because that is the terms of the Visa Waiver Program entry.

Senator BROWN. And why is it so long? It just does not make sense to me. I know when I go to other countries, we have to go through hoops to get into the country and then leave the country. I am a U.S. Senator.

Mr. BEERS. Ms. Jacobs, do you want to describe what the different classes are?

Senator BROWN. No, I do not need a lesson on classes. I am trying to pick up where Mr. Beers was zeroing in on. We have all these people here that are overstaying, and it does not seem like we are really zeroing in to either get them reclassified, helping them out if they want a different type of visa. What are the efforts? Am I missing something?

Mr. HEYMAN. Let me just say one thing that Mr. Beers did not get to say, which is that the number of 1.6 million will be down to zero in the next week or so, and we have committed to come back to brief you on that.

Senator BROWN. That is fair. See, I asked you the right question.

Mr. BEERS. No, I was going to get there. [Laughter.]

Senator BROWN. He is much quicker.

Mr. BEERS. The other half are now going through two databases to determine, first, whether or not there is any derogatory information that was available before or after they came into this country; and, second, whether or not they would be subject to the targeting rules that the Customs and Border Protection organization runs against people who are in this country. That will reduce the number from the remaining half to a smaller number who will be classified as persons of interest. The entire remaining number will be turned over to ICE with a notation as to who are the most prominent numbers, and as Mr. Heyman said, I am expecting a report of the completion of this process tomorrow. We will get back to the Committee as quickly as possible, at Senator Lieberman's request.

Chairman LIEBERMAN. Thank you, Senator Brown. We will have a few more questions each and then let all of you go back to work.

Let me pick up where Senator Brown ended and where I ended on my first round. So we understand now what the Department has done to work through this backlog that existed of overstays, but let us talk now about what is the ideal state we are looking forward to in terms of an exit system, as I mentioned, so we do not develop another backlog and so we have a much more contemporaneous understanding of where people are after they come into the country, or at least did they leave when they were supposed to leave when their legal right to be here ended.

And as I mentioned in my opening statement, Mr. Kean and Mr. Hamilton, when they testified before us, again called for a comprehensive biometric exit system. And then GAO recently reported that the current biographic system continues to be full of problems.

So take a minute, because this really is important to the Committee, and tell us what the biographic system is, how it works, and whether you agree that we should be working toward a comprehensive biometric system, how that would work, and what you need to get there as quickly as possible.

Mr. BEERS. Mr. Heyman, do you want to start with the enhanced biographic that you have been working on?

Mr. HEYMAN. One of the challenges that we have had with overstays historically is that the biographic information is not easy for us to reconcile in terms of who is here and who is not here.

Chairman LIEBERMAN. So what does "biographic" mean?

Mr. HEYMAN. "Biographic" means the name, date of birth, the textual information that we gather on departure of an individual.

Chairman LIEBERMAN. So we recorded it when they came in?

Mr. HEYMAN. We got it when they came in, from the passport information.

Chairman LIEBERMAN. Right.

Mr. HEYMAN. And we get it when you leave.

Chairman LIEBERMAN. Right.

Mr. HEYMAN. And so we actually have real-time biographic exit, but the question is, over the last several years, we have been trying to improve the ability and the integrity of that data so that we can actually be sure that when we think somebody has left, they have left, or when we think they have overstayed, they have overstayed. And we have not had that until recently.

Over the last several months, Mr. Beers' folks have been doing deep dives into the data on a pilot basis to see if we cannot get better integrity and be able to do a better job of actually knowing real-time when people have left using the biographic analysis. And the answer is we think we can. And the result of that is that once we complete the backlog and we can do real-time biographic, that will help us in the near term—in fact, we are doing that now—be able to accurately assess overstays on a more real-time basis.

Chairman LIEBERMAN. So that makes sense in that when you come into the country, not only do you give the biometric data by putting your fingerprint down, but there is passport information, so that is in the record. And when you leave the country, that is in the record, and presumably that is not a complicated data entry matter to find out who has not left after the date at which their visa expired, right?

Mr. HEYMAN. Correct.

Chairman LIEBERMAN. So what you are saying is you think you can do better at working that biographic system.

Mr. HEYMAN. Correct.

Chairman LIEBERMAN. Are you still thinking about going over to a biometric system?

Mr. HEYMAN. Yes.

Mr. BEERS. Sir, we have not stopped thinking about this. As you know, we have run some pilot programs and some cost estimates.

Chairman LIEBERMAN. Right.

Mr. BEERS. The last cost estimate we had, the lowest cost estimate we have ever had, was $3 billion over 10 years. We are still looking for a more cost-effective solution to close the gap between the enhanced biographic that we are currently working with and the validity of the biometric exit.

Chairman LIEBERMAN. Is biometric, just for the record, largely a fingerprint or——

Mr. BEERS. Although we can come up with another solution, but that is what we have spent our time looking at.

Chairman LIEBERMAN. Right.

Mr. BEERS. That is what the $3 billion estimate was associated with.

Chairman LIEBERMAN. Do you conclude that it is more effective to have a biometric than a biographic system?

Mr. BEERS. Sir, I have said before, before this Committee, that in the end that is the highest fidelity system that we would have. The question that we are faced with is whether or not the highest fidelity system is sufficiently cost-effective in the current budgetary environment, and that is why we have asked S&T to look hard and see if they can come up with perhaps even a new way to approach this problem. We do not have the results of that yet.

Chairman LIEBERMAN. That is important. So that is the first step, and it is a significant step. But let us say whether it is enhanced biographic or biometric, either way you are going to know, am I right, which of the people who have come into the country on a visa have overstayed the visa?

Mr. BEERS. Yes, sir.

Chairman LIEBERMAN. And then what do we do?

Mr. BEERS. That is where the visa backlog and the going-forward system is going to identify in near real time after they pass into the overstay status whether or not—as a result of the interrogation of the databases—they are persons of high interest because of some derogatory information or behavioral activities which I can talk to you more about in a classified setting. This information says that we ought to really pay more attention to this particular person, which is not to say that the other names will not go to ICE, but then ICE will have to decide with respect to whom. This goes back to Senator Paul's concern about focusing on the high-risk persons first, who the people that we would put in the high-risk category are in order to do that.

But the thing I want to tell you is that does not stop the recurrent vetting that we will have to continue to do to ensure that, as I said earlier, if more information comes in at a later point in time, even though it is historical information, we want to get that information to the investigator.

Chairman LIEBERMAN. So this is a question really for ICE, but maybe you know. This is a very labor intensive, but I presume in the ideal system that on the day somebody's name popped up as their visa has expired and they should have left the country and we do not have a biographic or a biometric indication that they have, that somebody would begin to look for them, presumably at their last known address or whatever. But I assume that is not happening now? Leave aside for a moment they are screening—which is a very good move, of course, to try to set a kind of priority based on activities or suspicions. But right now what does ICE do about all those people who overstay their visas?

Mr. BEERS. Let me focus on the persons of interest because that will give you a sense of what they can do. They can look, as you quite correctly said, at the last known address. They would look to see what other evidence there is in any databases that they might be able to access that would provide some further information about where that person was or what that person was doing. So they would look, for example, at if they got a driver's license. They would look for whether or not the person had a phone. They would

look for whether or not the person had a credit card and other kinds of indicators that are publicly available information which would help establish location so that they could zero in on that person. So the front end of that is preparing the case, and then the back end of that is for the ICE investigator to go out and actually try to find the person.

Chairman LIEBERMAN. To the best of your knowledge, is ICE able to do those kinds of checks on everybody who overstays their visa?

Mr. BEERS. Certainly not on everybody who overstays their visa, no, sir.

Chairman LIEBERMAN. So we have to get to a point where a person who comes in on a tourist or student visa, or any other kind of limited-time visa, worries that the odds are that they are going to be apprehended. I fear that right now the odds are that they can probably avoid detection, whether they are here for evil reasons or, as most of them probably are, just here to work and make a living. Either case is a violation of our law.

My time is up. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Assistant Secretary Heyman, there is some good news in your testimony on the issue of applying new data to these holders now, and I believe your written testimony says that to date, for this fiscal year, DHS has revoked 782 visas using this process of using the kinds of new information that Under Secretary Beers has referred to to revoke visas. And this brings to mind the Abdulmutallab case where there was a lack of understanding that the Christmas Day bomber even had a U.S. visa.

Assistant Secretary Jacobs, this is an issue that we talked about extensively in April of last year when you testified, and we talked about the misspelling of Abdulmutallab's name by embassy officials which resulted, at least initially, in the failure to realize that he held a U.S. visa.

Now, your testimony today says, "For visa applications, we employ strong, sophisticated name-searching algorithms to ensure matches between names . . . and any derogatory information. . . ." And then you go on to say something which puzzles me. You said, "This robust searching capability, which takes into account variations in spelling, has been central to our procedures since [the] lookout system checks were mandated following the 1993 World Trade Center bombing." So I am trying to reconcile your testimony today when you say that we have had the capacity to check for variations in spelling since we instituted these procedures many years ago following the 1993 bombing and what happened in the Abdulmutallab case.

Ms. JACOBS. Thank you, Senator. Actually, we are dealing with two different databases and so that explains the difference. What we created after the original attack on the World Trade Center was our lookout system, or what we call CLASS, where we develop many algorithms that allow us to search for names using what we call "fuzzy logic," which basically means you can misspell a name, if there are differences in how, for example, an Arabic name is transliterated. Our CLASS system for many years has had these sophisticated abilities or algorithms so that no matter what you

put in, it would bring up several different results so that you could look through to see if it applied to the applicant.

That search capability was not available in our Consular Consolidated Database when the name was put in for Mr. Abdulmutallab, and so one of the changes that we made after the attack Christmas 2009 was to make the same fuzzy logic search capability available in our Consular Consolidated Database, and we tell everyone now when they are searching for names or any other information that they have to use what we call our person finder search, which involves this fuzzy logic.

So today if that name was misspelled and put into the Consular Consolidated Database, it would, in fact, have hit on this name and several others that came close.

Senator COLLINS. But earlier today you and Under Secretary Beers indicated that there are still some problems with databases and their capacity to interrelate. So give me your assessment—it seems like we have all these databases, and the FBI example of the fingerprints is a perfect example. That just seems like such a logical place to look. So what is your assessment of the compatibility of all of these databases that are critical to our ability to protect against terrorists traveling to this country and overstaying visas or all of the other problems that could cause us to have someone in our midst who could do harm?

Ms. JACOBS. Thank you. That is a very good question. I would say that one of the issues that we focused on after 9/11, in addition to the need for Federal agencies to do a better job of data sharing, we also looked at all of the stand-alone systems that each of us use and tried to figure out how can they speak to each other.

When DHS was creating US–VISIT—frankly, I think US-VISIT is one of the best examples of how agencies can partner together because one of the first things we did was to make sure that our visa information was made available to the inspectors at the ports of entry through US–VISIT. When people come in, they are able to pull up on their screen the information from our visa database. They are able to look at the fingerprints that we collect. It is interoperable. It works extremely well.

That goes for the FBI as well. We had some issues in the very beginning, but we have worked through those, so that all of our visa applicants are checked against a DHS fingerprint database and the FBI database.

It is true that there are some agencies who did not participate in this exercise that we all underwent early on after 9/11. The Department of Defense, for example, has still some stand-alone systems where certain information resides. Now, DOD does or is supposed to share any information on known or suspected terrorists. That should come into these other systems that do talk to each other. But to the extent that there are other people in those stand-alone databases that are not automatically checked against, something might be missed.

What we are doing now in the case of Iraqi refugees and SIV applicants, for example, is we check all of these existing systems, but in addition, we are now doing separate checks against DOD systems. And DOD is working very hard to make their system interoperable with our systems.

So there is still some work to be done, that is absolutely true, but I think certainly between the State Department, DHS, and FBI, it really is a good-news story.

Mr. BEERS. Could I add something, Senator?

Senator COLLINS. Yes, Under Secretary Beers.

Mr. BEERS. We would have interviewed the individual in question when——

Senator COLLINS. When he got here.

Mr. BEERS [continued]. He got here, based on the information that was available. Given the new system that we had, it is quite possible that he would have been denied boarding overseas. But we did not have that system in place until after this event. Had that person's visa been revoked, he would have been denied boarding. That is a system that we have worked out between ourselves in terms of how to do that because just because the State Department revokes a visa does not mean they have any way of telling the person that the visa has been revoked. They would have to find the person and tell him that, and the person would still have the visa in the passport. So that is another improvement that we have had since then by being able to keep people off the planes rather than having to wait until they get here before we get a chance to talk to them.

Senator COLLINS. That is absolutely critical, but another aspect of the Abdulmutallab case that was most disturbing to me was that the derogatory information about Abdulmutallab from his father to our embassy officials did not trigger the revocation of his visa and, thus, block him from boarding the plane in the first place. And I know improvements have been made so that supposedly that would not happen today, but that still is so troubling to me that he was not listed on the watchlist and preferably on the No Fly List, but also that his visa was not revoked. That was a pretty gaping hole.

If I could just ask one more very quick question, it is about the Visa Security Program, which we have talked about many times. We have talked about it over and over in our April hearing in 2010 and again today in both of our opening statements, and we have talked about how DHS and the State Department have identified 57 posts as high risk. But I want to go to a subcategory of the high-risk posts, and that is, the GAO tells us that 20 are characterized as the highest-risk posts. So why aren't we covering at least those 20? We have 19 posts covered now, but 5 of those are not in the highest-risk posts.

I understand that there are limited resources, but I do not understand why we would not assign DHS officers to the highest-risk posts first.

Mr. HEYMAN. So the process for deciding how to get a visa security officer to a post includes a joint risk assessment between the State Department and the Department of Homeland Security. We do this on an annual basis, and that is where that ranking comes up. So we have a sense of priority, not necessarily need per se, but it is a priority ranking.

Last year, as you know, we had additional funding for visa security officers, and we expanded the program to the extent we could. When we consult with the State Department either because of an interest on our part to enhance the visa security and to provide

Visa Security Units or when the State Department talks to us, that has to be jointly done, and it has to also be done with the posts. The ambassador has the final say of who can come to post and whether there is even space available.

So some of the things that we go through are: (A) what is the priority; (B) what are the resources available; and, (C) whether there is even space available. We continue to review that. Last year, I think quite effectively, in the 19 posts we had about 815,000 applicants for visas of which 105,000 required further review and 1,300 we recommended be refused. And so there is quite a big tempo on that, and we, as I said, will continue to review that both in terms of resource availability and priorities.

Senator COLLINS. Well, thank you for that response. It still troubles me very much if an ambassador is blocking the implementation of this critical program in any of the posts that have been ranked the highest risk. Security ought to be No. 1.

Mr. HEYMAN. In the past year there have not been any blockings of that nature that I am aware of, but that is one of the considerations that goes into it, whether a post has space available.

Senator COLLINS. Thank you.

Ms. JACOBS. Senator, if I may just add very quickly just two things. One is that for the existing VSUs and any future ones, we did sign an MOU with ICE earlier this year that really defines very well the roles and responsibilities of the visa security officer, the consular officer, and then if we have someone from diplomatic security helping in the consular section. And so we are very pleased about that. It is something that Assistant Secretary John Morton and I worked on together, so we know that for the current ones and any ones in the future that those roles and responsibilities are clearly defined.

And I would also like to add that, in addition to the reviews that are done by ICE overseas in these Visa Security Units, in fact, ICE here in Washington has access to all of the same visa information that is available to the ICE officers in the field. This comes through our Consular Consolidated Database. And it is true that every day they are reviewing that information right here in Washington, and if they see cases of concern, they notify the post. And these are posts where we do not even have VSUs. So they are able, in fact, to do that review back here and have input into cases.

Senator COLLINS. Well, either the program is needed or it is not needed. If you can do it remotely, then maybe we should be questioning the whole program. But if the program is needed, it does not make sense to me that only 9 of the 20 highest-risk posts have DHS officials stationed there to review visas. That just does not make sense to me.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins. I agree with you. Senator Paul.

Senator PAUL. Thank you.

On the underwear bomber, not only does it perplex me we did not take his visa away, why didn't we send the Nigerian police over to his house? His dad is there reporting him. Why wasn't someone looking for him? I mean, it is really doing police work. That is what I think more of this has to be about, good police work, rather than

focusing on just database searches and all that. And we have to take away visas. But when someone's dad comes and says they are a threat, the police should have gone over to the guy's dorm or his house or tried to find him somewhere in Nigeria. I am not aware that there was an active effort looking for this man before he came over here.

But I wanted to get back to the FBI list and the idea with the Bowling Green terrorists and the fingerprint on the bomb. You said we need to ask the FBI, when they came in in 2007, or 2009, there was no FBI database or something called the Terrorist Screening Database? That did not exist in 2007 and you did not have access to that?

Mr. BEERS. Sir, we had access to that. This particular file, this particular print, was not in any of the databases that the FBI had to which we have access.

Senator PAUL. That makes it clear. So the problem really was not that you did not have access to lists. They did not put the information on the list. I know nobody wants to talk about it. They just want to say it is better. But there was a problem then. There obviously was a problem because we let somebody in with fingerprints on a bomb. It really sounds like the problem mostly originates in the FBI, that they did not put this information into the correct database, because you do not now have new access to a new database. They are just doing a better job, supposedly, getting the information into the database? Am I correct?

Mr. BEERS. Yes, sir.

Senator PAUL. Were either of these two Bowling Green terrorists on any kind of watchlist?

Mr. BEERS. At the time that they were put into the asylum system, no.

Senator PAUL. So that would have all occurred after the whole investigation started?

Mr. BEERS. Unless the information had been available before, and then they would have been on a watchlist.

Senator PAUL. All right. That is all I have. Thank you.

Chairman LIEBERMAN. Thanks, Senator Paul.

Thanks to the three witnesses, Under Secretary Beers, Assistant Secretary Jacobs, and Assistant Secretary Heyman. Frankly, thanks up front for all that you and your predecessors have done to create this quite remarkable and, I think, largely effective system we have for preventing terrorists from traveling into the United States to attack us. And I guess I would say thanks for the work that we are going to continue to do together to try to close the gaps that continue to exist. It has been a very informative hearing, and I thank you very much for your participation.

We will keep the record of the hearing open for 15 days for additional questions and statements.

With that, the hearing is adjourned.

Mr. BEERS. Thank you, sir.

[Whereupon, at 12:34 p.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11: IMPROVING EMERGENCY COMMUNICATIONS

WEDNESDAY, JULY 27, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:01 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Collins, and Brown.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning, and I welcome the witnesses particularly and urge you to feel comfortable and take your seats. It is good to have you here.

This is another in a series of hearings that Senator Collins and I and our Committee have been doing as we approach the 10th anniversary of 9/11 to essentially evaluate what lessons we learned from that tragic day and what we have done to act on those lessons. One of the revelations of that day was the enormous gaps in our emergency communications capabilities. The fact is that on 9/11, a lot of first responders could not coordinate their rescue efforts because they could not talk to each other.

As one New York City fire chief told the 9/11 Commission, "People watching on TV certainly had more knowledge of what was happening a hundred floors above us than we did in the lobby [of the World Trade Center]." And that proved fatal because many firefighters inside the Twin Towers did not hear the call to evacuate.

In its report, the 9/11 Commission said, "The inability to communicate was a critical problem at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, State, and Federal levels remains an important problem."

As a result, the 9/11 Commission recommended the Federal Government take the lead in helping State and local governments establish interoperable communications systems.

A year after the Commission issued its report, Hurricane Katrina slammed into the Gulf Coast, and we saw there the relevance of the critique of the 9/11 Commission not just to man-made disasters, such as a terrorist attack, but to natural disasters as well. Be-

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00167 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

cause on the Gulf Coast, as a result of Hurricane Katrina, the lack of interoperable communications was compounded by an inability of many communications systems to operate at all under those circumstances.

Phone lines, cell towers, and electrical systems were destroyed by the storm, knocking many communications systems offline and making it impossible at times for many first responders and government officials on the Gulf Coast to talk to each other.

Governor Haley Barbour of Mississippi memorably said, "My head of the National Guard might as well have been a Civil War general . . . because he could only find out what [was] going on by sending somebody."

Today at this hearing, we are going to assess what progress we have made and what gaps remain in making public safety communications more interoperable and more operable in a crisis.

In assessing what has happened since 9/11, it is important to remember, I think, that planning and funding decisions for emergency communications traditionally have been splintered across over 55,000 public safety organizations across our country that operate on many different bands of radio spectrum.

But as we look back almost 10 years now, I would say that significant progress has been made in bringing these varied organizations together.

The Implementing Recommendations of the 9/11 Commission Act of 2007, which was the second wave of legislation from the 9/11 Commission report, which, again, I am proud to say originated in our Committee, created the Office of Emergency Communications within the Department of Homeland Security to coordinate with State and local governments in addressing the many challenges that come with trying to create interoperable communications systems.

With assistance from the OEC, each State and territory has now created a communications interoperability plan and has appointed a State interoperability coordinator, and I am pleased to say that these officials meet face to face twice a year and are in ongoing communication about how to improve interoperability.

That is very significant because not so many years ago, it was not always clear who the point person in each State was when it came to interoperability or if there actually was such a point person.

In 2008, OEC issued the National Emergency Communications Plan to establish clear goals for improving interoperability, and to ensure that the plan is more than just a piece of paper, OEC has been testing to see if its goals are being met. In 2010, OEC tested 60 urban areas to see if they could demonstrate that they could rapidly establish communications among agencies from all levels of government in the event of an emergency. I am pleased to say that all 60 urban areas met the goals set by OEC. They are now working with the States to test the capabilities of the more than 3,000 counties across the country.

Investments in many State and local communications systems, which have been significant, supplemented by over $4 billion in grant funds from the Department of Homeland Security, have significantly enhanced voice communications and interoperability of

voice communications over what they were a few years ago. In this regard, it is comforting to report that one of the greatest success stories actually comes from Louisiana, which has used State money, DHS grants, and stimulus dollars to build a single, statewide radio communications system that provides daily voice communications to more than 60,000 Federal, State, and local users.

This system, incidentally, proved its worth during the evacuation of almost 2 million people before Hurricane Gustav in August 2008 and again after the Deepwater Horizon oil spill when the system was the backbone for establishing interoperable communications among the various first responders in the Gulf States. So that is real progress.

But despite such progress in voice communications, we still have failed to fulfill the recommendation of the 9/11 Commission to set aside a portion of the radio spectrum and dedicate it to create a coast-to-coast, interoperable, emergency digital communications network for first responders. We have the opportunity to do that right now, and I think we need to seize it.

Currently, public safety agencies transmit on narrow slices of non-contiguous spectrum that cannot handle the kinds of large chunks of data available to the average smartphone user.

Turning over a large contiguous slice of the broadband spectrum, which is known as the D Block, to public safety would give our first responders a 21st Century communications system with equipment that could share information with any other department anywhere in the Nation. Right now, as one of my staff members put it, one of my more eloquent and colorful staff members, the average firefighter or first responder does not have the capability that the average teenager with a smartphone has, and that really is unacceptable.

If we close this gap, as an example, firefighters could get digital building diagrams from the local building department as they approach a burning building so they know the floor plan and exits before they go in.

Paramedics could send a patient's vital signs to the emergency room so doctors and nurses would know what they were dealing with before the patient arrived.

A police officer at the scene of a crime could take electronic fingerprints and immediately compare them to Federal, State, and local databases. Or the officer who gets a partial read of a license plate could immediately tap into a database to help determine who owns the car and whether they have outstanding warrants against them.

Senator McCain and I have sponsored legislation to set aside the D Block for first responders, and we are committed now to working with Senators Rockefeller and Hutchison, Chairman and Ranking Member of the Commerce Committee, who have reported similar D Block legislation out of their Committee.

But I will note that Senator Reid, to bring what we are talking about that began 10 years ago right down to today, in his proposal to end this debt ceiling crisis that approaches, that we are in the middle of—and D–Day is next Tuesday, apparently—has included auction money from the spectrum as contributing to diminishing the deficit, but has allocated $7 billion of that for these purposes.

For reasons that are not clear to me yet—and we have to talk to him and his staff—that is $4 billion less than the Rockefeller-Hutchison bill and Senator McCain and my bill, and we want to see what is going on there. But all the authorizing language is now in Senator Reid's debt ceiling proposal, so perhaps one of the witnesses is either clairvoyant or has been tapping phones and emails and can predict better than Senator Collins and I can what actually will happen here in the next 3 or 4 days on the debt ceiling. But here all of a sudden—and we do not know whether this is in Speaker Boehner's proposal or not because we have not seen the language—we have the possibility of actually achieving this as a resolution of this larger crisis in the next week, and that would be great.

In this 10th year after 9/11, adopting this legislation I think is one of the best things to do to show that we have learned the lessons from 9/11. The bottom line is, our first responders need a nationwide network giving them the most modern broadband capabilities.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, as you were talking about the debt crisis, I could not help but think that it would be good if something positive came out of this debacle that we find ourselves in.

Good morning to all of our witnesses. Mr. Chairman, I am not sure that you realize that we not only have a witness from the State of Maine with us, but that the Connecticut witness hails from Milo, Maine.

Chairman LIEBERMAN. I would like to say I knew that. [Laughter.]

Mr. Varney, this does not put your credibility in doubt with me at all. [Laughter.]

It only enhances your credibility.

Senator COLLINS. I was just going to say, be careful there. This is a big plus and now gives me great confidence in what Connecticut is doing as well as what Maine is doing.

The effectiveness of emergency communications has emerged as a concern due to the failures that occurred in the wake of the 9/11 attacks and the Hurricane Katrina disaster. As both of these catastrophes demonstrated, the lack of reliable communications before, during, and after a disaster can cost lives, worsen damage, and slow response operations.

Not only did the 9/11 attacks represent a "failure of imagination," as the 9/11 Commission found, they also revealed the inadequacy of communications equipment, technology, and systems. The 9/11 Commission report cited many problems with communications among firefighters on September 11, 2001, and found that the technical failure of the fire department's radios was a "contributing factor" to the loss of firefighter lives, albeit not the primary cause.

Incredibly, when Hurricane Katrina struck in 2005, we saw exactly the same kinds of problems that we had witnessed 4 years earlier in the 9/11 attacks. Emergency personnel had incompatible equipment even within the same Louisiana parish. Major commu-

nications problems arose when towers and electronic equipment were destroyed, 911 centers were rendered inoperable, and the FEMA Mobile Emergency Response Systems were overwhelmed.

A FEMA official who was in New Orleans after Hurricane Katrina estimated that the lack of effective communication at the Superdome reduced FEMA's effectiveness by 90 percent.

This Committee conducted an in-depth investigation into the failed response to Hurricane Katrina and detailed the various communication failures associated with that storm. Although there are numerous examples, one of the most notable assessments that sticks in my mind is the one that the Chairman has already cited, and that was from Governor Haley Barbour when he said that it was as if he were back in the Civil War because he had to send messengers to communicate. He noted that he did have helicopters instead of horses, so it was a little faster, but the same concept.

When seconds and minutes are important, communications systems must be both operable and interoperable so that first responders can talk to each other and coordinate their operations. We never again want to see individuals on rooftops pleading for help that may be delayed because of an inability of responders to communicate. We must be especially sensitive to the ability to communicate with the most vulnerable in our population, such as children, the elderly, the homebound, and those with special needs.

As the 10th anniversary of 9/11 approaches, how first responders communicate with one another and how Americans receive emergency information remain challenges.

Public safety officials clearly should have access to state-of-the-art, interoperable communications equipment to use during emergencies. But we must also be sure that resources are invested carefully and that an effective and efficient structure is established to manage emergency communications. That, too, was a problem after Hurricane Katrina. There was not a command-and-control structure in place that could be implemented even if the equipment had been there and had operated. And that is why plans and systems must be tested during State, regional, and national level exercises.

Today, the Committee will examine the progress made during the past decade and explore what more needs to be done. After Hurricane Katrina, Congress created the Office of Emergency Communications within DHS, which developed a National Emergency Communications Plan, stood up Regional Working Groups, and established goals to measure progress.

The Chairman and I also created an Interoperability Emergency Communications Grant Program to support State plans. This program has supplemented other Federal, State, and local investments. According to CRS, as much as $13 billion in Federal funding has been spent on emergency communications during the past 9 years.

What exactly do we have to show for these investments? Are we making sufficient progress? Is the money being well spent so that we are better prepared for the next major disaster?

I know from my experience in my home State of Maine that a great deal has been done to increase the ability of first responders to communicate with each other. Notably—and I want to ask our witness, the head of the Maine Emergency Management Agency,

about this today—our State has been working with Canada to ensure that first responders across our more than 600-mile international border can communicate with each other in an emergency. When you look at the border of Maine with Canada, there are communities on both sides, and they often have assistance packs to allow for help when there is an emergency, but they have to be able to communicate as well.

The investments, training, new equipment, and planning clearly have produced some successes. For example, in recent testimony, the FEMA Administrator testified that interoperable communications were effectively used after the Joplin, Missouri, tornado and that the success of State and local responders reduced the burden on the Federal Government.

Another issue is the importance of effective communication with the public before, during, and after an incident. This is an issue that has been of great interest to the Chairman and me. We have talked about who would be the most credible spokesperson, who should get information out to the public, particularly if there were a nuclear disaster and the instruction might well be to shelter in place, not to flee. Much like the communication among first responders, the communication between officials and the public is vitally important and can save lives. I will soon introduce legislation, on which I look forward to working with the Chairman, to strengthen the Nation's public alert and warning system.

But, again, today I want to thank all of our witnesses for being here and especially to welcome our two witnesses from the great State of Maine. [Laughter.]

Chairman LIEBERMAN. Thank you. Thanks, Senator Collins.

Before we get to the first witness, apparently there is a public safety meeting of some kind in Washington, and we are honored to have, in addition to our witnesses, a number of first responder officials. I am going to call out some names that I have, and I apologize if I have missed anybody, but I thank you for your service and for being here:

Chief Harlin McEwen, who is Chairman of the International Association of Chiefs of Police Communications and Technology Committee; Sheriff Paul Fitzgerald, President of the National Sheriffs Association, and Sheriff of Story County in Iowa; Chief Gregg Riddle, incoming President of the Association of Public Safety Communications Officials International; Chief Al Gillespie, North Las Vegas Fire Department, incoming President of the International Association of Fire Chiefs; Chief Gregory Frederick, President of the Metropolitan Fire Chiefs Association, from the Louisville Fire Department; Chief Charles "Chuck" Dowd, Deputy Chief for Communications of the NYPD, we welcome you back. You have become not quite a regular but a frequent visitor here—and Kevin McGinnis, State Trauma Coordinator and Chief of Mobile Health Services from——

Senator COLLINS. From the great State of Maine.

Chairman LIEBERMAN. Oh, yes. [Laughter.]

We have an ongoing routine. Anyway, we are honored to have all of you here.

Our first witness at the table is Greg Schaffer, who is the Acting Deputy Under Secretary, National Protection and Programs Direc-

torate of the U.S. Department of Homeland Security. Thanks for being here, and please proceed with your testimony.

TESTIMONY OF GREGORY SCHAFFER,[1] ACTING DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SCHAFFER. Thank you, Chairman Lieberman, Senator Collins, and distinguished Members of the Committee. It is a pleasure to be here today to talk about the Department of Homeland Security's efforts to support emergency communications and the emerging capabilities of our State, local, tribal, and Federal resources in that space.

Today's hearing is just the latest in this Committee's consistently strong support for first responder emergency communication needs, a tradition that includes the passage of the Post-Katrina Emergency Management Reform Act and the statutory creation of the Office of Emergency Communications.

There are three offices within the National Protection and Programs Directorate that directly support emergency management and interoperable emergency communications capabilities:

The Office of Emergency Communications, which really helps create the foundation for first responders and public safety officials at all levels of government to talk to each other during an emergency.

The National Communications System works in times of disaster to ensure that there is priority communication capability for Federal, State, local, and other officials, as well as creating the ability, along with FEMA, to restore those communications when they are disrupted by a man-made or natural disaster.

The third office, the Office of Infrastructure Protection, works across all sectors of critical infrastructure to ensure that owners and operators of our most critical infrastructures have the ability to restore capabilities and that they are provided with capabilities to communicate with the Federal Government during a time of disaster.

I am happy to elaborate in all of these areas and answer your questions, but I would like to focus on some success stories, as has been noted.

There has been significant progress made in the area of emergency communications through investments in planning, governance, training, interagency coordination, and technology support. As a result of those efforts and work in that area, we do have a better situation than we have had in the past, but there is still certainly more progress to be made.

One example is the April 20, 2010, Deepwater Horizon drilling rig explosion, which released enormous amounts of oil, as we know, in the Gulf of Mexico. As noted, the Louisiana Wireless Information Network was used as a major backbone for communications for emergency responders after that incident. Indeed, within 24 hours, the LWIN mobile tower capability was launched to Mobile, Alabama, and voice communications were established between area

[1] The prepared statement of Mr. Schaffer appears in the Appendix on page 599.

commands in Robert, Louisiana, and two unified command groups in Houma, Louisiana, and Mobile, Alabama. Within 48 hours, technicians were working with the Louisiana Department of Public Safety to connect the statewide radio system in Mississippi as well as the Orange Beach Fire Department radio system in Alabama to LWIN through various motor bridge devices that allowed for effective communications all the way from the Texas-Louisiana border to the Florida Panhandle.

Louisiana also issued over 200 portable radios from their State's cache of 600 to allow the U.S. Coast Guard to immediately establish voice interoperability, and then within a week, radio systems in Austin, Houston, and Harrison Counties in Texas were added to the system through interoperable RF subsystem interfaces, which extended the network, which was now called Gulf WIN, all the way to central Texas.

This rapid connectivity of multiple systems was possible due to the integration of communications unit leaders at all levels of government, and Louisiana, Mississippi, and Orange Beach granted access to individual radio IDs in all of these systems, which essentially allowed the use of one handset to talk through all of the networks.

That network is still in operation today, and as we come into hurricane season, it is good to know that we have a capability that really connects the entire region.

As a second example, as was noted by the Chairman, Joplin, Missouri, experienced an F–5 tornado that, while tragic, did display new capabilities or enhanced capabilities of our communications networks. The investments in standards and in grant funding for interoperable communications equipment and training really did yield measurable improved results of our communications capabilities. The city of Joplin's 10-channel trunked radio system experienced heavy use, but it continued to operate throughout the incident response, and the establishment of an incident command capability reduced the confusion that can occur after an event of this kind.

Indeed, in the very week before this event occurred, there was a training by DHS, a national-level exercise, with many of the responders participating and being brought up to speed on the way to respond in a mock earthquake scenario. So these examples really show that we have made critical strides in strengthening the overall security and national preparedness of the communications systems over the last decade.

The public safety community, while enhancing their capabilities on the mission-critical voice side, they do not have all of the capabilities that they need from a data capability perspective. The availability of new technologies in the Long Term Evolution space—4G mobile capabilities to allow them to use data as mission critical as we do with voice capabilities today—is something that we believe must be realized for the community to bring greater operability, interoperability, and capability across the board.

In order to realize that vision, the Administration is fully committed to working with Congress to ensure the passage of legislation that meets the critical needs of the public safety community to have broadband communications capabilities. The fact that Con-

gress has been working across several committees, multiple jurisdictions, including Chairman Lieberman, Chairman Rockefeller, and Senator McCain, we believe is a sign that we can indeed get this accomplished.

We will continue to work with you to achieve this goal. We thank you very much for the opportunity to testify this morning, and we look forward to ensuring that in the aftermath of the 9/11 attacks of 2001, we are taking enormous strides to make sure that emergency communications capabilities continue to advance.

Chairman LIEBERMAN. Thanks, Mr. Schaffer. That was a good beginning.

Next we go to the frequently mentioned Michael Varney. Senator Collins, you will be interested to hear that Mr. Varney brought with him from Maine not only enormous capability but a tremendous work ethic. He is here today as the Statewide Interoperability Coordinator from Connecticut, but he is also the Director of Statewide Emergency Telecommunications at the Department of Emergency Services and Public Protection, the Vice Chairman of the National Council of Statewide Interoperability Coordinators, and the Chief of the Ellington, Connecticut, Volunteer Fire Department.

Thank you for all your public service.

TESTIMONY OF MICHAEL D. VARNEY,[1] STATEWIDE INTEROPERABILITY COORDINATOR, CONNECTICUT DEPARTMENT OF EMERGENCY SERVICES AND PUBLIC PROTECTION

Mr. VARNEY. Thank you, Senator. Chairman Lieberman, Senator Collins, and distinguished Members of the Committee, I would like to thank you for allowing me the opportunity to provide testimony on this important topic.

As the Senator indicated, I am the Statewide Interoperability Coordinator for the State of Connecticut in addition to serving as the Vice Chairman of the National Council of Statewide Interoperability Coordinators.

Being a local first responder and serving in the capacity as a fire chief, I can truly appreciate the efforts put toward solving the nationwide interoperability problems and have seen their positive impact directly in the field.

Close to 10 years ago since the attacks of September 11, 2001, a priority for States has been improving emergency responder communications capabilities. Public safety responders need the ability to have the most accurate, reliable information and to be able to communicate directly and instantaneously with their assisting and supporting responders.

Interoperability of public safety communications takes significant coordination to solve and is being addressed by the creation and use of Statewide Interoperability Coordinators. In each State and territory, there is a designated SWIC responsible for a variety of critical planning and coordinating functions, guided by the initiatives outlined in the National Emergency Communications Plan and the Statewide Communication Interoperability Plans, all of which were not coordinated through a specific designated office prior to 2001.

[1] The prepared statement of Mr. Varney appears in the Appendix on page 611.

In Connecticut, our Statewide Public Safety Interoperable Communications Committee has representatives from each planning region within our State—law enforcement, emergency medical services, fire departments, and key State and Federal response agencies. The abilities and relationships that are leveraged by this group have been very successful in our efforts to improve interoperability of public safety communications within the State of Connecticut.

Each of the Nation's Urban Areas Security Initiative sites developed a Tactical Interoperable Communications Plan. Connecticut used this framework to continue to create TIC Plans for all of the additional regions in our State. This effort was possible because of the Interoperable Emergency Communications Grant Program. Since the TIC Plans have been developed, they have been used in the field by local practitioners to successfully plan for and respond to events and emergencies that involve multiple disciplines and jurisdictions.

In early June when tornados struck southern Massachusetts, the Connecticut fire service was requested and responded with significant assets, which were coordinated quickly and efficiently between the two States due to prior planning and exercises made possible through the IECGP-funded TIC Plan process.

SWICs serve as members of the National Council of Statewide Interoperability Coordinators, which was established in 2010 to assist State and Territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices. As a SWIC, I have received excellent support and engagement by the DHS Office of Emergency Communications. Their technical support and coordination activities have proven invaluable to our efforts in Connecticut. Their outreach activities through SAFECOM and the NCSWIC have listened to our concerns and priorities and adapted their programs to make them relevant.

As I mentioned earlier, the IECGP funds such as those used to create TIC Plans in Connecticut have been critical to the SWICs to provide funding that ensures that federally funded projects align to strategic plans and to implement and report on the NECP goals, allowing DHS to measure progress in emergency communications capabilities nationwide.

In a recent survey of SWICs conducted in June, we found that over one-third of the SWIC positions were funded in whole or in part by this grant program. The elimination of this funding and reduction of related homeland security grant programs will have a direct impact on the sustainment of the many programs put in place to increase interoperable communications.

We support the commitment to develop and deploy a nationwide interoperable wireless network for public safety that the Administration has put forward in the President's Wireless Innovation and Infrastructure Initiative. Many of our issues are captured within the Rockefeller-Hutchinson bill, and we are very appreciative of Senators Lieberman and McCain's leadership and the Homeland Security and Governmental Affairs Committee in their work to reallocate the D Block for public safety use. This leadership will ensure successful completion of this very important milestone.

While maintaining their traditional land mobile radio systems, our public safety agencies are increasingly using commercial broadband systems to support their missions. We have been relying on off-the-shelf broadband systems using laptop computers in vehicles and communication devices such as BlackBerrys and smartphones for remote data communications. Although the present commercial broadband devices have some functions that go beyond public safety communications devices, they lack the ruggedness, reliability, and direct device-to-device connectivity of traditional public safety radio systems. In other words, the commercial networks do not provide the public safety control, mission criticality, and capacity needed for their mission.

The Statewide Interoperability Coordinators believe that the creation and support of a wireless broadband network for public safety is critical for interoperability and to allow first responders to communicate and do their jobs as safely and efficiently as possible. We appreciate your ongoing support to make this nationwide network a reality, and the NCSWIC is very appreciative of the initiatives supported by the Homeland Security and Governmental Affairs and Commerce Committees to create a national public safety broadband wireless network.

As Senator Lieberman indicated in his comments earlier, right now my son and daughter have more broadband capability than my firefighters do while responding to emergencies every day. This is a unique time to solve this problem and create a nationwide public safety wireless broadband network. We look forward to working with you and your Senate colleagues to pass this law to meet public safety's needs for interoperable communications, a key recommendation of the 9/11 Commission Report.

In conclusion, I again would like to thank the ongoing tremendous support and activity by your Committee to increase interoperable communications throughout the United States. The Federal investment to support interoperable communications over the past few years will continue to show its value in saving lives and protecting property while our Nation's first responders work together to respond to emergencies and disasters in our homeland.

Thank you again for this opportunity to testify, and I would be pleased to answer your questions.

Chairman LIEBERMAN. Thanks very much, Mr. Varney, for that excellent statement.

Now we will go to Robert McAleer, who is the Director of the Maine Emergency Management Agency and who, as far as I know, was not born in Connecticut. [Laughter.]

Mr. MCALEER. No, sir. New Jersey.

Chairman LIEBERMAN. Welcome.

TESTIMONY OF ROBERT P. MCALEER,[1] DIRECTOR, MAINE EMERGENCY MANAGEMENT AGENCY

Mr. MCALEER. Senator Lieberman, Senator Collins, Members of the Homeland Security and Governmental Affairs Committee, thank you for the opportunity to come before you this morning. My

[1] The prepared statement of Mr. McAleer appears in the Appendix on page 616.

name is Robert McAleer, and I am the director of the Maine Emergency Management Agency.

I would like to address the issue of communications interoperability as it relates to the State of Maine and, in particular, some of the accomplishments we have achieved since 2001, our work that is currently in progress, and existing gaps that need to be addressed.

By New England standards, Maine is a large State, roughly equivalent to the rest of the New England States combined. It is mostly a rural State with vast areas of very limited population and some very rugged terrain. Maine is also not a wealthy State. These factors have made improving interoperability a challenge.

Maine, however, has been fortunate to receive a significant amount of Federal funding, for which we are very grateful, to support our efforts. We estimate that approximately $9.5 million or 25 percent of our Homeland Security, Public Safety Interoperable Communications, and Interoperable Emergency Communications Grants funds have been dedicated to improving communications just since 2007. We have used that funding to leverage whatever local funding municipalities have generated to make notable improvements.

One advantage that we have had throughout this process is that the vast majority of our first responders use VHF radios that transmit and receive on similar frequencies.

Because of the overwhelming similarity in equipment statewide, our challenge has been to replace old or worn-out equipment and to acquire new equipment where there was none or to replace equipment that simply was inadequate to meet our current needs.

In addition to acquiring a large number of modern radios for our first responders, we have completed a significant number of major projects. An attachment to my testimony contains a detailed compilation of the projects since 2003, examples of which are as follows: $107,000 to upgrade communications systems throughout Sagadahoc County and complete their narrowband transition; about $200,000 to upgrade the communications infrastructure for the Hancock County Sheriff's Office; $500,000 for the bulk purchase of narrowband-compliant fire pagers; and $350,000 to support a countywide microwave communications project in Cumberland County. The State has also acquired four large mobile command vehicles that have state-of-the-art radio, cell phone, internet, and satellite capabilities for use in incident coordination. In multiple instances, these vehicles have served as dispatch centers when fixed facilities were out of service. We have also provided support for communications vehicles in over half of our counties.

The State has established radio caches at crossing sites along the U.S.-Canada Border for use by first responders moving across the border to ensure adequate interoperable equipment is available. Each county now has portable repeater antennas that can be deployed to remote areas where coverage may be minimal or to boost signals that may otherwise be blocked.

We have been able to move our EOC from a facility that was generally inadequate to a new facility and provide the new EOC with equipment that meets virtually all of our communications needs. Our court system and law enforcement agencies now have

access to a data broker system that enables almost instant access to the various types of critical information.

The majority of our law enforcement and even some fire departments now have mobile display terminals in their vehicles, which in many cases provide a better communications capability than standard radios.

We realize that interoperability is not just a matter of acquiring equipment. In many instances, process and training also bring gains. Along those lines, we have established a Memorandum of Understanding with the owners of six statewide frequencies to allow incident commanders to request dedicated use of those frequencies to establish and coordinate communications at an incident.

We have also dedicated a significant amount of time to communications unit leader training. This training helps us ensure that there is sufficient expertise available at a large event to ensure that the correct agencies are speaking on the correct channels.

We have worked with our counties to ensure that they have up-to-date detailed countywide communications plans to identify all of their communications assets, to ensure that their procedures are adequate, and to identify any gaps.

Our border with Canada has presented a unique challenge. To meet that challenge, we have been conducting a series of cross-border communications working sessions with our local, State, and Federal partners on both sides of the border. These sessions are helping us better understand our differences and plan for how we can overcome those differences when needed.

In addition to these workshops, Maine, with the support of our Canadian partners, applied for and received a Border Interoperability Demonstration Pilot grant. Out of 21 applicants nationwide, Maine was one of only seven awardees. We are using the almost $4 million provided by this grant to significantly reduce communications gaps along the border and establish a single common frequency that will be available for use by first responders from both sides of the border.

Finally, the State of Maine is investing $50 million of State funding to essentially rebuild and expand the infrastructure backbone of the State's communication system. When this project, MSCOMMNET, is completed, the State will have a series of 42 interconnected transmission towers that will replace infrastructure that has reached or passed its useful life expectancy, provide enhanced coverage, and increase redundancy. Of note is that part of the tower build-out is a joint effort between the State and our Customs and Border Patrol partners. We believe this may be the first such partnership in the Nation. Included with this project is the replacement of virtually all State-owned portable and mobile radios.

In general, Maine is in a relatively healthy position with regard to interoperability. Through the concerted efforts of many people and the judicious use of available resources, we have been able to accomplish a great deal. And we have witnessed those accomplishments coming into play during real world events. There is, however, more work that needs to be done.

First and foremost in our view is the requirement to meet the FCC narrowbanding mandate. While the initial estimates of the

cost to meet this requirement were staggering, we have dedicated a major portion of available Federal funding to the requirement as well as a concerted effort to encourage local communities to recognize their own responsibility to invest in the solution. Because we will be able to reallocate many of the State radios that are being replaced as part of MSCOMMNET, we believe that our first responders will be ready on January 1, 2013. We remain concerned, however, about communities that are not meeting the National Incident Management System compliancy requirements because we cannot assist them with Federal funds.

We believe firmly that during an emergency situation if we do not have solid communications, then we will have no coordination. We will only have chaos. For that reason, building a solid communications capability has been a priority for the State for a number of years. Further strengthening of that capability and sustaining what we now have will be priorities moving forward.

That concludes my testimony. I would be pleased to answer any questions you might have. Thank you.

Chairman LIEBERMAN. Thank you very much for that good report.

Finally, we have Charles Ramsey whom we knew here for a long time as Chief. We welcome back now Commissioner of the Philadelphia Police Department and President of the Major Cities Chiefs Association.

Commissioner, it is an honor to have you here. Thank you.

TESTIMONY OF CHARLES H. RAMSEY,[1] POLICE COMMISSIONER, PHILADELPHIA POLICE DEPARTMENT

Mr. RAMSEY. Thank you, sir. Good morning, Chairman Lieberman, Senator Collins, and all invited speakers and guests. Thank you for this opportunity to discuss a critical issue affecting all public safety and law enforcement organizations across our country and our ability to serve the public. Having had 42 years in law enforcement, I have witnessed many important changes in emergency communications across police departments in three cities: first in Chicago for 30 years, then as Chief of the Metropolitan Police Department here in Washington, DC, for 9 years, and now as Police Commissioner in Philadelphia for the past 3½ years. I also have the privilege of serving as the President of the Major Cities Chiefs Association and the Police Executive Research Forum, both of which are members of the Public Safety Alliance.

The PSA is a coalition of the leading national public safety associations that represent every law enforcement, fire, EMS, emergency management agency, and first responder organization in the country. I am here on behalf of first responders across this country to thank you, Mr. Chairman, and Senator McCain for sponsoring S. 1040, the Broadband for First Responders Act of 2011. And we hope that you will also continue to work closely with Senator Rockefeller and Senator Hutchison of the Senate Committee on Commerce, Science, and Transportation and sponsors of S. 911, the SPECTRUM Act, which was recently voted out of Committee for consideration by the Senate.

[1] The prepared statement of Mr. Ramsey appears in the Appendix on page 627.

These bills fulfill an absolutely critical need. They allocate the D Block to public safety, provide the necessary funding to build out and expand the nationwide broadband network, and establish a governance structure in cooperation with State and local authorities.

Since September 11, 2001, like many other jurisdictions around the Nation, the Philadelphia region worked diligently to ensure adequate local, State, and Federal coordination for emergency communications. We established an Interoperable Communications Committee within our Southeast Pennsylvania Regional Task Force. Representatives from the five counties in the Philadelphia UASI, as well as seven additional regional counties from New Jersey, Delaware, and Maryland, comprise this task force. I would also like to take the time to thank Committee Member Senator Tom Carper for his assistance in strengthening homeland security in our region.

Let us be very clear in our mission: A terrorist attack or a major catastrophic event knows no municipal, State, or Federal boundary. Emergency preparedness spans across lines and demands that law enforcement and public safety organizations across the country plan and coordinate their responses.

And as you mentioned in your opening remarks, Mr. Chairman, we have an extremely valuable opportunity in front of us to meet our needs in emergency communications. Seamless interoperability can only be achieved through a dedicated public safety nationwide broadband network. The allocation of the D Block for public safety organizations, with adequate capacity, control, and funding, is the only proposal that will meet the challenges and demands that we confront. As President of MCCA and PERF, I am here to support this solution, which serves law enforcement and public safety organizations and, most importantly, helps to protect the American people in the best way possible.

Commercial networks are not designed to serve our public safety needs. Past experiences with major national disasters have demonstrated that these networks are not interchangeable with dedicated public safety networks. There are fundamental differences in the architecture that go to the heart of public safety communications. The Public Safety Alliance will strongly oppose any legislation or resolution that supports auctioning the D block. Public safety becomes both less public and less safe if we auction any part of the D Block to the highest commercial bidder.

We need the up-front funding to jump-start the investment and build out of the network and to attract and encourage commercial interest and competition. We will partner with the private sector to leverage and make maximum use of the existing infrastructure, while managing operations locally through a national governance structure.

This Committee, the House Homeland Security Committee, the House Energy and Commerce Committee, and the Senate Commerce, Science, and Transportation Committee have all held numerous hearings over the past 2 years on the proposed public safety spectrum and the nationwide broadband network. Congress has asked many good questions, and hopefully you now have the information you need to make an informed recommendation.

Our first responders, who put their lives on the line every day, must have the resources that they need to do their jobs more efficiently and effectively, armed with real-time data, video, and other critical information. We can only accomplish this goal if we have the latest in mobile broadband technology that is fully interoperable on a local, State, and Federal level. The ability to share mission-critical information nationwide to coordinate and plan our response to emergencies depends on having this capability.

I would like to thank all the Members of the Committee for your continued time and commitment to finding a solution that will meet the communications needs of our first responders and will best serve the American people. What Congress decides now will dictate the future of our emergency response capabilities. Ten years after 9/11, we urge you to make the decision that will finally establish a dedicated nationwide public safety broadband network.

I am happy to answer any questions that you may have, sir. Thank you very much.

Chairman LIEBERMAN. Thank you, Commissioner. Very helpful, very good testimony.

We will now do 7-minute question rounds for each of us.

Mr. Schaffer, let me begin with some of the monetary implications of what we are talking about since we are all focused at every level of government on the cost of government, and let me suggest a point of view to you and ask you to react to it.

Currently, because public safety agencies operate on so many systems, equipment costs can be quite high since there is not much economy of scale for manufacturers. For example, I gather that a handheld set for a police or fire officer can cost around $5,000.

So I wonder whether an advantage of building a D Block network might be that it would create that economy of scale that would drive down costs, which, of course, would be very helpful to Federal, State, and local governments. What do you think?

Mr. SCHAFFER. Senator, thank you. That is certainly one of the hopes of this proposal, that, in fact, by aggregating and getting public safety together on a single standardized set of equipment based on the commercial standard that is being deployed by virtually all of the commercial carriers, we create an opportunity for an economy of scale level that has never been seen before for the public safety community.

We would love to see a situation where handsets cost a couple hundred dollars rather than several thousands dollars as they do today.

Chairman LIEBERMAN. And you think that is an achievable goal?

Mr. SCHAFFER. Based on the interactions that we had with the manufacturing entities over the last year, the economies of scale are much better with a national network of this sort where you have millions of potential customers buying from the same pool rather than a city or a small entity.

Chairman LIEBERMAN. Let me give the other witnesses the opportunity to comment on that from your own experience. Obviously, all of us would like to see the cost of the equipment go down, but is there anything that you want to reflect based on your own experience in acquisition on this question? Mr. McAleer.

Mr. MCALEER. We are paying significantly less for our radios up in Maine. However, I think that is probably because of the nature of the radio that we are talking about here. These may be P25-compliant radios, whereas the radios that we are buying at this point just to meet the narrow banding requirement are not P25. We realize that there are certain issues there, but that is the best that we can do. So our radios are from $300 to $500, and we have found that even at the county level, when there is bulk buying, prices do go down.

Chairman LIEBERMAN. Right. Let me ask, beginning with Commissioner Ramsey, if you could elaborate a bit, again, from your own on-the-ground experience, on the kinds of uses you would make of broadband technologies if the D Block is allocated to public safety.

Mr. RAMSEY. Thank you for that question, Senator. I was listening to some of the testimony earlier, and the issue of the oil spill came up and how we were able to put together a network that would allow for some interoperability. And that is a good bridge, but it is not a permanent solution because as a police chief, I have to use a network every single day for a variety of reasons, not just an emergency that may come up on occasion. So not only do we have the need for voice interoperability, but we also have computers in all of our cars. We need to be able to get information out to those cars. We need to be able to get information from those cars. We need video. We have video in our vehicles. We have video in our city that needs to be monitored. You mentioned during your opening statements fire departments rolling to the scene that need blueprints for buildings. Well, if we have an active shooter in a building, we will need those same blueprints for our SWAT team. If they have video inside that building, we will need to tap into that in real time so we can see exactly what is going on: Where are the hostages? Where are the shooters? All those kinds of things need to be able to take place.

Aside from that, more and more we are using video conferencing with our courts, with our prosecutors to save time in moving prisoners from one point to another. There are just so many different uses, and the way in which technology is evolving so rapidly, who knows what we will need 10 years from now? So we have to have the capability to expand and to grow as our needs grow.

I have been around a long time. Call boxes were still in use when I started my career, and the radios were still in police cars. So, it is just unimaginable to me what could possibly take place over the next four decades in law enforcement.

Chairman LIEBERMAN. That is true.

Mr. RAMSEY. So we need a solution now that is not only going to meet our current needs, but our future needs as well.

Chairman LIEBERMAN. Well said.

Mr. McAleer, do you want to add anything from your own perspective about other possible uses of the D Block if it is allocated to public safety?

Mr. MCALEER. Sir, that would go to a level of technical information that I am not comfortable dealing with.

Chairman LIEBERMAN. Mr. Varney.

Mr. VARNEY. In addition to what was said earlier by you and all of the witnesses, access to facility information, chemical data and processes, utility services, HVAC systems within the building would be able to be accessed by the responding units to try to mitigate incidents, in addition to the access to inside-building cameras and surveillance systems, which certainly would add to the safety and enhancement of operations.

Chairman LIEBERMAN. That is very interesting. Right now you cannot do any of that easily.

Mr. VARNEY. No. Certainly not easily.

Chairman LIEBERMAN. That is an interesting thing. You might be able to access into an inside-the-building camera system.

Mr. VARNEY. Certainly all of those things could be put in place with access to a broadband system such as that.

One of the other important things we would want to do in the future as the next generation 911 systems are built throughout the United States, we would want to be able to get the information that is sent from the public in the form of data, video, or pictures when they report incidents to the responders while they are en route, which gives them a greater situational awareness of what they are getting into. More data make better decisions.

Chairman LIEBERMAN. That is a very interesting point because we are now all accustomed to viewers sending video into TV stations, for instance, from the scene of a natural disaster or a crime scene. And that capability to pick those up is not there at this point.

Do you want to add something, Mr. Schaffer?

Mr. SCHAFFER. Yes, sir, Mr. Chairman. I think it is also important to recognize that there will be uses that we cannot even imagine today. Five years ago, no one could have imagined what we have in smartphone technology and a very large universe of applications that have been developed in a very short period of time for the commercial sector. I think once this capability is available to our public safety community, we will see the opportunity for a whole range of new capabilities that we cannot imagine or articulate today. We have great examples of what the art of the possible is now, but what will come when they have access to the spectrum and capability will be even beyond what we might be able to articulate now.

Chairman LIEBERMAN. Absolutely right. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Schaffer, in your testimony, you detailed much of the progress that we have been able to make, and that is encouraging. You also said there is a great deal more work to be done.

It is disappointing to me, therefore, that the President in his budget chose to terminate the funding for the Interoperability Emergency Communications Grant program. That was a program that is near and dear to our hearts because it was our initiative and was included in the 2007 homeland security law.

Given that we all agree that more work needs to be done and given what you have heard today about the use that the money has been put to and how it has made a big difference in the State of Maine, for example, why would the President choose to terminate

that program? It is a pretty modest program in the scheme of things, but it has been really helpful to States.

Mr. SCHAFFER. Yes, Senator. I think that the opportunity to have money flow into emergency communications capabilities is certainly still there through a number of grant programs and the focus through, for example, the Emergency Communications Preparedness Center of developing grant guidance that applies across 40 different grant programs that steers those grant dollars in the direction of the kind of interoperable communications capabilities that you and the Chairman have supported in the past.

So I think the focus has been on general grant opportunities and making sure that all of those grants across the entire range of opportunities are being directed in a way that is consistent and that can advance the ball with respect to what we are doing in land mobile radio today.

Senator COLLINS. I agree with the goal of having more consolidation of grant programs, but the fact is, if you do not have a targeted stream of funding that is aimed at improving interoperability and sustainability of emergency equipment, you are not going to reach the goal that we all agree is necessary. So that is something that I know the Chairman and I have already communicated to the Appropriations Committee on, but it is something that I really think is short-sighted given that every first responder group always says that interoperability and sustainability of equipment is such an important goal. And it cuts across every State, every kind of first responder. They all need that to be effective.

So I hope that is something we can continue to work with the Department on. I do not mean to put you as much on the spot as if Secretary Napolitano were here, but I did want to mention my concern about the termination of that program. It has not been in operation for very long, and to terminate it before we reach the goal—someday we will be able to terminate it—seems to me to be premature.

Mr. McAleer, I want to ask you more about the program that you have with Canada. I think this is fascinating and far-sighted. Having grown up 20 minutes from the Canadian border in northern Maine, I am so aware of the fact that there are mutual aid packs where our firefighters on the Maine side of the border assist Canadian firefighters and vice versa. We have a wonderful Federal program called Operation Stonegarden where our law enforcement works with Border Patrol officials, which has been a force multiplier as well. And when you come from a border State, whether it is the Northern border or the Southern border, you cannot ignore the fact that you are going to need your partners on the other side of the border.

So tell us a little more about what the goals are of the grant programs that you are participating in right now.

Mr. MCALEER. The primary cross-border grant program that we are dealing with is the Border Interoperability Demonstration Project Program, and that is a program that was sponsored by the Federal Government that we won the grant for and is helping us increase our cross-border communications with both our New Brunswick partners and our partners in Quebec. And our grant ap-

plication was supported very strongly by partners in Canada at the local and provincial levels. So they are very much in favor of this.

Currently, both New Brunswick and Maine use VHF channels, and so we are able, when necessary, to use common channels. What we are trying to do is formalize that process so that those channels are loaded up on both sides—we have Canadian channels loaded in our radios, and our channels loaded in their radios—because as it is right now, we have worked with the Border Patrol, and the first responder communities come across very quickly, and there is no stopping them. When they get there, they need to be able to communicate. In those instances where we do not have the channels in the radios, we have those radio caches. We have about 12 caches at sites along the border already that we established with State Homeland Security Grant funds, and we are looking to increase that with the BIDP funds, and then increase our transmission capability in four of our counties to cover some of those vast gaps that we have out there in the wilderness.

Senator COLLINS. Several years ago, before you assumed your current position, there actually was a problem with the Maine State troopers having interference from the New Hampshire State troopers when they were using the same channels in Southern Maine, and I recall helping to secure some funding to sort that out.

Is that still a problem, are you aware?

Mr. MCALEER. I have not heard of that problem recently, Senator.

Senator COLLINS. I think that has been fixed, but that, too, shows that you can have interference even between two bordering states that can interfere with the ability to respond.

Mr. MCALEER. Absolutely.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins.

Senator Brown, timely appearance. If you would like to proceed with questions now, we would welcome them. If not, of course, I could fill a few moments.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. You are going to filibuster a little bit? No, I am all set. I was at another hearing. We are having a Veterans Committee hearing upstairs, so I apologize.

Chairman LIEBERMAN. No, not at all. Thanks for coming by.

Senator BROWN. I have been getting periodic updates.

Chairman LIEBERMAN. It is all yours.

Senator BROWN. Thank you.

Mr. Schaffer, in Commissioner Ramsey's testimony, he notes that disasters do not stop at State borders, and witness testimony has highlighted efforts at the State level, such as the Statewide Communications Interoperability Plans. Considering that a disaster in the New England region and the Northeast corridor in general could include multiple jurisdictions, what is DHS doing to ensure regional coordination across State lines? And, obviously, we have had some pretty interesting weather in Massachusetts. As recently as yesterday, another tornado hit. So I think it is a timely question.

Mr. SCHAFFER. Yes, Senator, no question, it has been a very active season from a weather perspective, and, of course, the hurri-

cane season is just getting started now, so we are certainly focused on these issues.

There are several things the Department has been doing to ensure regional interoperability and coordination. Of course, the National Emergency Communications Plan is the foundation for much of that work. The development of Statewide Communications Interoperability Plans, the appointment of Statewide Interoperability Coordinators who have banded together in many regions to form regional coordination groups to work these issues, all are moving us in the direction of better capability to be able to cooperate across multiple jurisdictions. The development of standards like the P25 standard are advantages as well. If we are all buying to the same standard, we have a better opportunity to have our equipment work. But we are still in a situation where it does end up being a project when people arrive on the scene to get all of those radios tuned to the right frequencies, to the right interoperability channels, and have them operate the way we like, which is why the Administration believes that the development of a national public safety broadband network based on the same technology across the board will improve things even further.

Senator BROWN. Thank you.

Mr. Varney, I certainly want to thank the State of Connecticut for its help in Massachusetts, and I noted that when the tornado struck, Connecticut Fire Services were there to quickly coordinate.

What made the coordination possible from a State and local perspective?

Mr. VARNEY. It comes from years of work across the border coordinating efforts.

Senator BROWN. Do you have something in writing, or is it just a custom and courtesy thing?

Mr. VARNEY. I think it works from relationships that start initially, but then it becomes more formalized over time. In Connecticut, what we have done to work with our bordering States is we put together a system where whenever an interoperability system or sub-channels is activated for an event in-State or near a State border, all of our area States are notified immediately of that, which creates coordination and alleviates the issue of interference when multiple people are trying to use the same interoperable channels. And through the years, we have worked closely on the borders with our fellow SWICs in the regional States, in our regional interoperable committees, as Mr. Schaffer indicated, so that we talk and formalize those issues where we know we are going to cross borders that happen on a regular mutual aid basis, and when things escalate to a larger basis, we can quickly coordinate those assets because we know the types of information that would be needed and the types of equipment that would need to be moved across the border.

Senator BROWN. So if there was a larger catastrophe, God forbid, what do you think the greatest challenge would be in handling a more widespread disaster?

Mr. VARNEY. The greatest challenge is that coordination effort. As was mentioned earlier today, the way that public safety is working in Connecticut and New England is a patchwork of many different frequencies and many different systems, so in order for us

to handle a large-scale event in any of the States, we have to bring in some pretty technical pieces of equipment and expertise through the COML and COMT trained personnel to patch these systems together, where if we had a nationwide single system that was standards-based and completely interoperable from the beginning, it would speed up that effort and make it less complicated for those problems to be solved.

Senator BROWN. Thank you.

Commissioner Ramsey, although Connecticut is right next door to New York City, Philadelphia is within a couple hours of it and within 3 hours of Washington, DC. It is conceivable that—and God forbid a disaster happens—a terrorist strike or something could impact your city or vice versa. Do you feel confident that proper coordinating frameworks are in place to ensure seamless communications within the region?

Mr. RAMSEY. It is better than it has been within the region. We have done a lot in that particular area, but again, it is not a permanent solution like a nationwide public safety broadband network would be. We are right across the river from New Jersey, not very far from Delaware or Maryland. So we actually could be involved in something where multiple States would be involved in the same event. There we would have some problems in terms of interoperability of our systems. We could probably patch the voice communications, but transmission of data would be different, and that would be something that would present even more of a problem.

So I think that a lot of regions across the country have come together to work out solutions for their communications problems as a region, but major disasters that require going beyond that region is where we are going to have a problem. And if there were a terrorist event for example, when you look at how they tend to take place in other parts of the world, usually it is multiple locations hit simultaneously. So now you have a much wider problem than you had before. It is not just a regional problem. It is much broader than that.

We need to be able to have lines of communication, and in an earlier question that Senator Lieberman asked, one of the other things that would be operating on D Block would be our fusion centers. We have fusion centers around the country, but you now have to fuse the fusion centers because it is going to be necessary for New York to communicate and get information from Los Angeles or someplace else in a very timely and secure fashion, either Federal, State, or local.

So, we have done a lot in terms of trying to patch it up the best we can, but nothing that comes close to a permanent solution.

Senator BROWN. And one final question, Mr. McAleer. You came from a 30-year career—congratulations—in the Marine Corps. What lessons did you take from your time commanding operational elements in the Marines to your job now in regard to dealing with the communication issues before you?

Mr. MCALEER. Well, the one thing you learn right away with communications systems is, if you do not work with them, they will not work when you need them. So we try to drill with our communications as much as we possibly can. For instance, with our radio network that we have with our counties, we exercise three times

a week, and it is amazing how even with exercising that many times, we have radios that are down, towers that are down. If we were not doing that kind of work, that would come as a surprise to us when the time came.

We also look at redundancy. Where do we have gaps and where do we have single coverage and where do we have redundancy? Because it is also my experience that when you are under stress situations and radios are being used hard, those systems tend to go down as well. So you have to have backup systems.

So I think probably the two main things that we have learned are that you have to exercise it and you have to have redundancy, or it will not be there when you need it.

Senator BROWN. Good advice, sir. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Yes, thank you, Senator Brown. Thanks for coming by. I appreciate it.

Just a few more questions. Mr. Schaffer, I want to focus in a little bit on the Federal Government interoperability. As you know, several years ago the Department of Homeland Security and the Department of Justice embarked on a joint project with the wonderful name of Integrated Wireless Network, which was shortened to the acronym IWN, which could be stated "I win." Unfortunately, IWN fizzled as a governmentwide effort. I gather the Department of Justice has continued to pursue the project, along with the Treasury Department and the U.S. Park Police, and has recently built out a system to provide interoperability to the agencies mentioned within the National Capital Region.

However, DOJ got a very small amount of money in the continuing budget resolution, so I think it is probably going to make it hard for them to maintain their legacy radio systems let alone continue or expand IWN.

Meanwhile, DHS component agencies like Customs and Border Protection and Immigration and Customs Enforcement have continued to make their own investments in tactical radio systems.

So I wanted to ask you whether we are doing enough on interoperability of communications within the Federal system. In other words, can CBP and FBI talk to each other? Or I suppose in a more immediate sense, in terms of DHS, can the different components of DHS talk to each other over these systems?

Mr. SCHAFFER. Thank you, Senator. The components can talk to each other as a general proposition, but it is a project as it is with these jurisdictions. They have to use these interoperable channels, and they have to program those radios in order to be able to interoperate.

We are making several steps in the direction of ensuring better interoperability with the existing technologies today in a variety of ways. At DHS, we have a committee called the One DHS Emergency Communications Committee, which for the first time is coordinating across all of the components of DHS and looking at how we coordinate our activity in terms of our investment in communications technology. And that has developed into a strategy for our tactical communications across the Department with some pilot projects that are looking at doing things in a coordinated way.

At the same time, the Emergency Communications Preparedness Center is trying to coordinate across a number of departments and agencies, including DOJ, DHS, and several others that have significant roles in emergency communications, to think about how to coordinate their activity in areas like new broadband technology and developing joint requirements across Federal departments and agencies that can then be used in coordination with the public safety community as a national public safety broadband network is developed.

So there are several initiatives underway to try to further coordinate among the entities in the Federal Government, writ large, and specifically within the Department of Homeland Security.

Chairman LIEBERMAN. So the availability of the D Block would also help components of the Federal Government communicate better with each other? Is that what I am hearing you say?

Mr. SCHAFFER. I think that is absolutely true.

Chairman LIEBERMAN. Let me ask you one other question. We had discussed the Office of Emergency Communications and that it has been measuring progress at the local level in meeting the goals of the National Emergency Communications Plan. I wanted to ask you whether you plan on issuing any type of report card or public statement measuring the results, which thus far seem to be pretty good.

Mr. SCHAFFER. The results are good, Senator. As mentioned, the Goal 1 work showed that all 60 of the large urban areas were able to establish emergency communications within an hour, as was the intent with Goal 1 for planned events. We are in the process of working toward Goal 2, which is a much broader effort, 3,000 counties as opposed to 60 large urban areas. That will consist of getting reporting from the counties. We do not have the resources to go out and examine each county as we did with the cities. But we will get reporting from the counties, both in terms of their ability to stand up communications for events and a broad view of their capabilities from an emergency communications standpoint.

We try to balance the collection of that data and the development of reports in this space. Because there is voluntary reporting coming to the Department, we try to be careful about having a report card that may make it harder for cooperative efforts to get that information flowing to us. But we do aggregate the data and try to give some indication of where we are and whether progress is being made.

Chairman LIEBERMAN. Very good. I appreciate it.

Mr. Varney, you mentioned the response to the June tornadoes in Massachusetts as an example of improved coordination between governments, and Senator Brown mentioned it as well. I wanted to ask you to just give us a little more detail on how the response benefited from the planning and exercises that you have conducted in recent years.

Mr. VARNEY. It is one of those things that you plan and you put together an exercise for something you hope will never happen, but it just so happens that in our north-central Connecticut region, our emergency planning region, several years earlier, to validate their tactical interoperable communications plan, the scenario was such that a tornado went south to north through a very close area of the

State, which actually affected some correctional facilities in the notional exercise and went into Massachusetts. So as part of the validation of that effort that we put together to collect the data, to identify the systems and personnel that would respond to an event, bring everyone together to walk through a tabletop exercise, all funded through IECGP funds with technical support and assistance from OEC, we were able to bring people from northern Connecticut and that area of Massachusetts together as part of this exercise to share equipment and to talk about those resources, only to have several years later a very similar event happen in a very close proximity. Although it was not in Connecticut, we were able to leverage all of those relationships and expertise that we were able to put together several years earlier to quickly respond to and enhance the efforts to support their request.

Chairman LIEBERMAN. That is a great example of the benefit of planning. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

We have talked a lot today about the importance of communications among first responders. However, I do not want to slight the importance of warning the public prior to a disaster striking.

Maine has had, like many other States, an extraordinary run of violent weather this year. In northern Maine, there have been four tornadoes. I never remember that happening in my lifetime. And we have seen violent storms throughout our country.

So getting information to the public before disaster strikes helps to save lives, reduce property damage, and prepare people for what is coming. Early warning can truly make a huge difference.

I noted when I was home that the warning I received of the violent weather was across my TV screen, and I happened to have the television on, and it was the old-fashioned emergency alert system that we have had for as long as I can remember. And I could not help but think that most people probably did not have their television on, but they probably had their mobile phone nearby. They probably were on a computer on Facebook, or there are so many different ways to communicate today.

So I would like to hear your assessment on the importance of having a system that embraces today's technologies because we need to recognize that people get their information in different ways nowadays. We will start with Commissioner Ramsey.

Mr. RAMSEY. Well, that is a very good point, Senator. In our department, we text-message a lot of information out to the public now about crime issues. We are taking advantage of Twitter. We take advantage of Facebook. We have what we call reverse 911 where we are able to use telephone calls to certain specific areas of the city, if there is a burglary pattern or a con game that is prevalent in a particular area, and we can reach people and warn them and let them know. So from a police perspective, we use the technologies that are available to get information out to the public the best we can, recognizing the way things have changed—my son, for example, would rather text me than have me call. If I call him, he says, "Dad, why did you call? How come you just did not text me?" So, that is the world we are in now. And so to reach a population, I think you have to do all the above. It is not one in lieu of the other. You have to do them all because different groups of people

use different ways to communicate, and we have to be able to adapt very quickly to that and get information out as quickly as we can.

With regard to a point you made in your opening statement, I believe that one of the shortcomings in preparedness in this country is our preparing the communities on a consistent basis on what to do in the event of an emergency. As first responders, we can have the best plans in the world. If there are traffic jams and we cannot get to where we need to get too, it does not matter how good your plan was, you cannot get there to deal with the situation because if you have panic among the public—and a lot of that comes from just not quite knowing what to do—then that is a problem. And if the FCC set aside 1 hour a month for PSAs for different jurisdictions to do 30-second or 1-minute PSAs over and over again—and I do not mean airing it at 3 o'clock in the morning on the Psychic Network and all that—I mean in prime time, constantly reminding people of certain things that they need to do, then I think we will have a better prepared public, which makes us even more effective if we can rely on the public to do certain things in the event of an emergency.

Senator COLLINS. Thank you. Great response. Mr. McAleer.

Mr. MCALEER. Senator, I believe that we can to a certain degree dictate when and what we will transmit to the public, and I say "to a certain degree" because if we do not put out the right information at the right time, there are so many other sources of information out there that the public will go to those sources, and then we in emergency management tend to become irrelevant.

The thing that I think we cannot do is dictate how we put that information out. We have to remember that our citizens are our customers. We have to be able to communicate with them in the ways that they communicate. It is much like a guy owning a shop. If you walk in and I try to sell you a T-bone steak and you are a vegetarian, it could be the best T-bone steak in the world, but it is irrelevant. So we need to be very careful about that.

I think this applies both before events and during the response to events so that we become the center of information for the public. The challenge becomes, how do we afford to pay for that because the technology is out there that can do it, but as you get more technologically advanced, it costs more money.

On the other side, if we with our systems are chasing the emerging technology that is out there, we might always be in a race. So if we could develop some sort of industry standard so that there was a talk-back means or a talk-forward means as these new social medias are coming online, that would help us a great deal, I believe. Thank you.

Senator COLLINS. Thank you. Mr. Varney.

Mr. VARNEY. In Connecticut, of course, we maintain and we leverage the emergency alert system when it is needed. But in Connecticut, we have also invested significant State funds to put in a system for our local municipalities and dispatch centers to use, similar to a reverse 911 type of system, to alert citizens for any type of incident that a municipality believes that they need to be alerted to, and we make that available to all of the local municipalities.

So if somebody wants to sign up to have messages sent to them via text on their BlackBerry or they want it sent on traditional voice mail to their phone, they can opt in to do that, and we will send it in the mode that they have asked for. That is in addition to having all of the land-line phones into the system. In case of emergency, a message has to go out to have people shelter in place, as was mentioned before, or to evacuate. Those systems are in place in Connecticut, and I would think that as IPAWS and the alerting systems mature in the future, they would all become integrated.

Senator COLLINS. Thank you. Mr. Schaffer.

Mr. SCHAFFER. Yes, Senator, indeed, the Integrated Public Alert and Warning System really is designed to take advantage of some of the new technological capabilities of the smartphones and other devices that almost everyone carries today. We need to be able to alert people who are in a specific geographic area, not just people who sign up and give their zip code, because they may be traveling to another area on a given day and there may be people who are visiting Washington, DC—we have tourists right now from all over the country and all over the world. So this system is designed to give warnings to people who are proximate to a cell tower, who are nearby, as opposed to people who have signed up or people who live in a certain place. And that is an effort not of NPPD, my organization within DHS, but FEMA working with the FCC. That solution should come into initial operating capability within this year, 2011, and have expanded capabilities going out for Federal, State, and local officials being able to send those kinds of alerts and warnings to broadcasters through a variety of digital communications paths sometime in 2012.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins, and I thank you, all four of you, for your testimony today and obviously for what you do every day.

The bottom line is, I think you validated our preliminary conclusion before the hearing that we have made a lot of progress in the area of interoperability of communications among first responders since 9/11 and the operability, the robustness of our communications systems. We obviously have some gaps yet to fill, and if this D Block legislation can pass soon, that would be a giant leap forward in assisting you to do what we ask you to do for all of our communities and States every day.

So thanks very much. You have really helped to inform the Committee and also, I think, given some testimony that should give the public an increased sense of confidence and security in an age when, because of the unpredictability of the weather, not to mention extremist and terrorists groups, this kind of capability is very significant.

I had not thought to mention the terrible tragedy in Norway, and we are just beginning to understand what happened, but part of it was that—this goes back to what Senator Collins quoted earlier from the 9/11 Commission—part of the cause of 9/11 was a failure of imagination by which the Commission meant that we failed to imagine that anybody could try to do to us what the attackers did on 9/11. And, of course, I think this is exactly what people in Nor-

way are going through because of their shock that anybody would try to do what that individual apparently did, and therefore, their relative lack of preparedness to respond to that.

Anyway, we are in much better shape than we were 10 years ago, thanks to you and a lot of other people. We thank you for that.

Senator Collins, do you want to add anything?

Senator COLLINS. I just want to thank our witnesses. I think this was a very helpful update on an issue that we have been working on together for many years, so thank you for the work that you are all doing.

Chairman LIEBERMAN. Thank you. The record of the hearing will be held open for 15 days for any additional statements or questions. And with that I thank you again and adjourn the hearing.

Mr. RAMSEY. Thank you, Mr. Chairman and Senator Collins.

[Whereupon, at 11:34 a.m., the Committee was adjourned.]

DEFENDING THE NATION SINCE 9/11: SUCCESSFUL REFORMS AND CHALLENGES AHEAD AT THE DEPARTMENT OF HOMELAND SECURITY

WEDNESDAY, SEPTEMBER 7, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, presiding.

Present: Senators Lieberman, Akaka, Carper, Pryor, Collins, and Brown.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. Thanks to our witnesses for being here.

In 4 days, we will commemorate the 10th anniversary of the attacks of 9/11 and mourn anew the nearly 3,000 lives that were lost that day at the World Trade Center, the Pentagon, and on Flight 93, which, as we all know, of course, crashed into a field in Shanksville, Pennsylvania.

But we have already quite appropriately begun and will continue, I am sure, a look back at September 11, 2001, to both understand with the clarity of hindsight what that day meant in American history and to evaluate what our government particularly and our people have done since that time.

There is no question that, although I think we knew it then, we can certainly look back and say now that we understand that on that day, we were drawn into a war which is increasingly global. We hesitate to use the term "world war," but this is a war that is being fought by violent Islamist extremists against most of the rest of the world, including most of the Muslim world. That day's brutal attack, in my own opinion, in the clarity of hindsight, began that war, although, in fact, Osama Bin Laden had declared war in 1998 in statements he had made, and they had been attacking us for some period of time before that, including the World Trade Center in 1993.

But it really began that day, and in the days and months following 9/11/01, we in government set out with an urgent determination to reform the systems that had failed us. I think the more we knew about how September 11 happened, particularly informed

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00195 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

by the work of the 9/11 Commission headed by Tom Kean and Lee Hamilton, we learned a lot more. I came to the conclusion, although one will never be able to know with certainty, that 9/11 was probably preventable. As I look back and I think of all we have done to respond to our failures on that day, I think that if another group of terrorists attempted a similar attack on the United States today, we would prevent it, and that, of course, gives me great comfort and a sense of great gratitude for all that has been done by so many people in our State and local governments to work together to make sure we are better secured here at home than we were on 9/11/01.

We put into place measures that reorganized and reformed our government to prevent another terrorist attack on the United States. I know that there are some on this 10th anniversary lookback that are saying that we overreacted to 9/11, that it was, in fact, not just a substantive overreaction, but an expensive overreaction. Well, I do not agree. The most extraordinary bottom-line reality today is that as we look back over the last 10 years, as we all know, thank God and thanks to everybody who has worked so hard, there has not been another mass casualty terrorist attack on the United States by violent Islamists since 9/11/01. I do not think anybody would have predicted that on 9/12/01.

But we can say that today not because our enemies stopped trying. They have tried over and over and over again. But fortunately, our defenses, our intelligence, all the things that we have done, really have made us more secure. And, frankly, a couple of times, just to remind us that we continue to have work to do, we were just plain lucky, as in the two glaring cases of the Detroit bomber on Christmas Day on the airplane and the Times Square bomber, both of whose weapons, explosives, just did not go off. If they had, I think we would be looking back with a different sense of these past 10 years.

But overall, there is no question in my mind, we have been spared another catastrophic terrorist attack like the one on 9/11 not just as a matter of luck or coincidence but because of a lot of things a lot of people did. I am very proud of the role Members of this Committee across party lines played back then and continue to play in creating these new organizations and supporting them.

The first, of course, was the cabinet-level Department of Homeland Security, which we created to lead our efforts to prevent terrorist attacks within the United States, and I believe DHS has significantly contributed to our increased national safety. I am grateful that the report that the Government Accountability Office has issued today to our Committee as we move toward September 11, 2011, essentially agrees with that, and it is a positive report on the work of the Department of Homeland Security. It points to some work yet to be done, and then I think we would all agree with that, including people at the Department.

But the fact is that 10 years ago, no single agency and no single official was designated to lead the Federal Government's efforts to prevent terrorism or, for that matter, to adequately marshal the resources of the Federal Government to respond to natural disasters, not just terrorist disasters. Today, there is clarity about who is in charge, and that is the Secretary of the Department of Homeland

Security, and whose efforts that Secretary should be coordinating to prepare, respond to, and recover from disasters. That has made a tremendous difference.

I am going to put the rest of my statement in the record because I want to hear the witnesses.[1]

I simply want to thank Deputy Secretary Jane Holl Lute from DHS who is with us today, and Gene Dodaro, the Comptroller General of the United States, both to hear DHS's own evaluation of these past 10 years and the Comptroller General's on behalf of GAO.

And I repeat, I am heartened that the report that GAO is issuing today[2] concludes that, overall, the Department of Homeland Security has implemented most of its key missions and achieved most of its important goals, creating a foundation that will allow the Department to continue to move aggressively toward its full potential.

So we appreciate that very much and look forward to the testimony of our witnesses. Thank you. Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. First, let me thank you for holding today's hearing to review the first 8 years of the Department of Homeland Security, whose vital mission is to protect our Nation and our people.

After the attacks of September 11, 2001, President George Bush established the White House Office of Homeland Security and soon concluded that the Nation needed a more unified homeland security structure. We envisioned a department that would secure our borders, improve the security of transportation and critical infrastructure, meld homeland security intelligence from multiple sources, and work with first responders and law enforcement to deter, detect, prepare for, and respond to terrorist plots.

The law establishing the Department of Homeland Security was enacted in November 2002. Twenty-two entities and approximately 180,000 employees were merged into DHS. Not only was the new Department's mission a challenge, but so was simply unifying its email systems. Over the past 8 years, the GAO has repeatedly placed the Department on its High-Risk List. The GAO has issued approximately 1,500 recommendations and DHS has adopted only about half of them, although others are in progress. This July, DHS issued a self-administered report card noting considerable progress in achieving the goals set out nearly a decade ago to strengthen our security.

When it comes to our homeland security, however, we are only as strong as our weakest link. This week, as the Chairman has indicated, we will commemorate the worst attack ever on the United States. In doing so, we must ask ourselves some fundamental questions. Are we safer, or are we just safer from the tactics terrorists have already tried?

I think the answer is yes to both questions. We are far safer than we were on September 10, 2001. But terrorists continue to probe our vulnerabilities and attempt to exploit gaps in our security. We

[1] The prepared statement of Chairman Lieberman appears in the Appendix on page 641.

[2] The GAO report titled, "Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11," appears in the Appendix on page 689.

also face increasing threats from homegrown terrorists already within our borders.

Today, the GAO concludes that more than 8 years after its creation and 10 years after September 11, DHS has indeed made significant strides in protecting our Nation, but has yet to reach its full potential. The examples are many. TSA has strengthened airline passenger pre-screening, yet a young man recently was able to fly cross-country without a valid government ID and with an expired boarding pass that was not even issued in his name. At the other extreme, it bothers many Americans to see TSA screeners putting the very young and the very elderly through intrusive and in many cases unnecessary pat-downs.

Although DHS has bolstered the security of U.S. borders and identification documents, two Iraqi refugees associated with al-Qaeda were recently arrested in Kentucky. How a known bomb-maker whose fingerprints we have had on file for some time was able to enter our country on humanitarian grounds remains an unanswered and extremely troubling question. Are there other Iraqi nationals granted asylum who were involved in attacking our troops? The fact is, we do not know. We still await clear answers from the Administration, which must do more to ensure that all relevant databases are used so that we do not let terrorists and criminals into our country, much less grant them asylum.

I am pleased that the GAO found that our chemical facilities and seaports are safer, both priorities of mine and of this Committee.

The GAO indicates that DHS should make improvements in how it shares and manages cyber threat information. This is the key goal of comprehensive cyber security legislation that Chairman Lieberman, Senator Carper, and I have co-authored. The Department has also had its fair share and then some of management problems. Failures in expensive procurements have cost taxpayers billions of dollars and delayed much-needed technology.

Now, merging 22 agencies and nearly 180,000 employees is always going to be a challenge. If DHS is to become a truly unified Department, its employees in headquarters should not remain spread over 70 buildings and 40 sites. The lack of a consolidated headquarters inhibits communication, coordination, and cooperation among DHS components, and I know the Administration is working hard to consolidate the headquarters.

I also believe that there are efficiencies that can be gained by consolidating offices at the regional level, a recommendation made by former Homeland Security Secretary Tom Ridge. We should take a look at consolidating field office locations to reduce costs and improve coordination.

As this Committee will soon consider a reauthorization of the Department, it is important to discuss what experts inside and outside of DHS believe has and has not worked. We must even answer the fundamental question of whether or not we are safer because of the creation of DHS.

As has been noted often, the terrorists only have to get it right once. DHS and its partners have to be right every single time or we will suffer the devastating consequences of a terrorist attack. We are much safer than we were 10 years ago, but we must be tenacious in anticipating the changing tactics of terrorists. As the

successful decade-long search for Osama bin Laden proved, America's resolve is a powerful weapon against those who would seek to destroy our way of life.

Mr. Chairman, I appreciate the opportunity to review GAO's report with the Comptroller General today and look forward to hearing from Deputy Secretary Lute on how DHS can better fulfill its mission. Thank you.

Chairman LIEBERMAN. Thanks very much for that statement, Senator Collins. Deputy Secretary Lute, welcome back. How long have you been at the Department now?

Ms. LUTE. Over 2½ years.

Chairman LIEBERMAN. Right. So for 2½ years you have been on the scene, and the previous years, you were an informed observer.

Ms. LUTE. Yes, sir.

TESTIMONY OF HON. JANE HOLL LUTE,[1] DEPUTY SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. LUTE. Thank you, Chairman Lieberman and Ranking Member Collins, and distinguished Members of the Committee, for this opportunity to appear before you today to discuss the Department's progress in keeping our Nation safe from the range of threats that we face.

Mr. Chairman, you have my full written statement. I request it be entered into the record.

Chairman LIEBERMAN. Without objection.

Ms. LUTE. And I would like to highlight some of that statement here this morning. But first, Mr. Chairman, I would like to strike a note of remembrance of the lives and memory of those who were lost on 9/11/2001. I was in New York City that day. I will never forget it. None of us will ever forget where we were, how we felt, and how we came together as a Nation, determined in our resolve to never let that happen again, determined in the conviction, in the core belief that this country can protect itself. And nowhere has that commitment been stronger than in this Committee, Mr. Chairman, with you and certainly you, Senator Collins, and the other Members of the Committee, and your steadfast support for the efforts that we have been taking in homeland security.

I would like to thank our many partners in our effort to ensure the safety and security and resilience of our Nation. DHS plays a central role in that effort, but we rely on strong partnerships throughout all levels of government, law enforcement, private industry, and with the public. We view homeland security as a whole community enterprise and we are fortunate to have strong partners to help us meet our mission.

As I mentioned, Congress is an essential partner. Particularly this Committee has played an extraordinary role in creating and equipping DHS and the other institutions with the authorities and resources necessary to carry out programs to secure our country. You have carried forward the bipartisan spirit that marked the days after 9/11, and you have always held us accountable to maintain that spirit and achieve our missions.

[1] The prepared statement of Ms. Lute appears in the Appendix on page 647.

In the spirit of accountability, we are also very thankful for the hard work of our partners in GAO, and I say that sincerely. Along with DHS's Office of the Inspector General, GAO has audited and reported on the work of the Department and their work has helped inform us as we mature and grow as an organization.

As we approach this important anniversary of the 9/11 attacks, we are thankful, too, Mr. Chairman, for the commitment of the American people. Since 9/11, countless Americans have stepped up, whether in our military in Afghanistan, Iraq, or in other posts overseas; in our Federal agencies, including the Department of Homeland Security; and in our States, cities, tribal communities, and elsewhere, as first responders, law enforcement officials, reservists, and engaged citizens.

I take great pride, Mr. Chairman, as you know, in my service in the U.S. Army for the first half of my adult life. But I am equally proud of my service as a member of the Department of Homeland Security.

Great progress has been made at the Department and around the country since the Department was created in 2003. Today, we are a more capable Nation and a stronger Nation. We can detect threats sooner with better information and make adjustments more quickly based on real-time intelligence. Today, we know more about those who seek to enter our country, the levels of risk they might pose, and what is needed to prevent potential threats from reaching our shores. Our borders are stronger, enhanced by more personnel, technology, and infrastructure, as well as with stronger partnerships with States, cities, border communities, and our international partners around the world, especially in Canada and Mexico.

Our immigration laws, while in need of reform, are being enforced according to common sense priorities that we have set, which are to identify and remove criminals and those who are a threat to the American people. At the same time, we have strengthened our processes and systems for providing legal immigration benefits and services while ensuring the security and integrity of our immigration system.

We have also created a framework for ensuring our cyber systems, networks, and our critical infrastructure where none previously existed. As part of this effort, we enhanced our ability to protect Federal Government networks through better detection, reporting, and countermeasures. We have engaged cyber users at all levels, public and private, in our shared protection, and we have broadened our partnership with the private sector to protect our critical infrastructure and established a new regulatory framework to protect high-risk chemical facilities.

We have built a more ready and resilient Nation that is able to confront major disasters and emergencies in our States, cities, and communities. We have helped front-line responders become more equipped, better trained, and more unified under a new national response framework and incident command system, as you have noted. We have improved emergency communications and we have provided capacity building grants to support our Nation's first responders.

The response and ongoing recovery effort from Hurricane Irene is just the most recent testament to the robust capabilities that you have helped us build.

We have continued to integrate the Department of Homeland Security by advancing the work that began more than 8 years ago to refashion our homeland security enterprise and engaged a full set of partners in the protection of our Nation.

And finally, the Department's commitment to civil rights, the values of liberty, fairness, and equality under the law are embodied in all of the Department's programs and activities.

While we have been making much progress, Mr. Chairman, we know we must continue to improve. As the threat against us continues to evolve, so do we. Today, then, is an important opportunity to talk about some of our progress, which GAO notes in its report, and also to address some of the areas where there is more work to be done. I look forward to discussing this with you today so that we may build upon the foundation of security in place to address our future challenges, and with this Committee's partnership and support, continue to protect our Nation, our citizens, our freedom, and our way of life. Thank you very much.

Chairman LIEBERMAN. Thank you, Deputy Secretary Lute.

Now, we will hear from Gene Dodaro, Comptroller General of the United States, and I note for the record that Mr. Dodaro is accompanied by Cathleen Berrick, who is the Director of Homeland Security and Justice Issues at GAO. Good morning, and please proceed.

TESTIMONY OF HON. EUGENE L. DODARO,[1] COMPTROLLER GENERAL OF THE UNITED STATES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. DODARO. Good morning, Mr. Chairman, Senator Collins, and Senator Akaka. I am very pleased to be here today to discuss GAO's report on the various homeland security issues and progress made as well as remaining issues and challenges since the 9/11 event.

Our report reflects a summary of the work that we have done over the last decade. It also reflects the constructive approach we have tried to take in making recommendations to offer improvements and suggestions to the Department. We are pleased with the Department's response, although many things, as Senator Collins mentioned, are still in progress and need to be implemented. But, generally, I think we have had a good dialogue and it has enhanced their operations.

The bottom line of our report, as everybody has noted in their opening comments, is that a lot of progress has been made since 9/11. That has clearly been demonstrated. But there is work remaining to address gaps and weaknesses that will enable DHS to reach its full potential.

Now, on the progress side of the ledger, we have Secure Flight in place, a system that checks incoming passengers against ter-

[1] The prepared statement of Mr. Dodaro appears in the Appendix on page 660.

rorist watch lists. We have screening workforces deployed at 460 commercial airports across the country.

We have a biometric entry system now in place to be able to check those people entering our borders over time. We have also established and put more resources, as Deputy Secretary Lute mentioned, at the ports and along the borders, putting resources, equipment, and infrastructure in place over time.

There is also the Border Visa Security Program that has been put in place to have DHS work along with the State Department in screening visa applications at certain locations overseas. And we also have put in place an electronic authorization program for those entering under the Visa Waiver Program.

There has also been a range of plans and assessments that have been done on maritime security, surface transportation, such as rail and mass transit, that have laid an important foundation for assessments of risk.

I am also pleased that cyber security has been given increased emphasis in the National Infrastructure Protection Plan, and as the Deputy Secretary pointed out, FEMA has issued a national response framework and associated documents with that to address emergency preparedness.

Now, on the work remaining side, there are a number of significant issues and I would like to highlight a few this morning. There needs to be continuous improvement in the processes and technologies used in screening operations at airports, including coming up with a plan to ensure that the equipment for screening checked baggage meets the current requirements for detecting explosive devices.

While we have a very effective entry system, we still do not have an exit system in place, and I know that this is a very difficult task, but the overstays issue is significant. The estimates are between four and five million people in the United States are overstays. Of course, as we know, five of the 19 hijackers on 9/11 had overstay issues. This is something that is a big challenge but needs to be addressed going forward.

We also think that the Visa Security Program can be expanded so that DHS is working with the State Department at more critical high-risk locations, whether DHS staff are deployed abroad in countries or working remotely from here in the United States. That program has a lot of potential for being strengthened.

There also needs to be a practical approach to screening cargo and containers before they come to the United States. DHS has some important programs underway. Of course, there is the 100 percent screening requirement, but there are questions about its feasibility. We need a practical approach to address that issue.

Also, Senator Collins, as you mentioned, in the cyber security area, we have noted that there is a need for more timely and actionable alerts to the private sector and others so they can take action over time.

Also, we believe FEMA needs to continue to work to develop some metrics and a methodology to address jurisdictions' preparedness. I think the roles have been articulated, but there is really not a clear assessment of preparedness levels of various jurisdictions yet.

There is also a need to effectively implement the global nuclear detection architecture and to strengthen abilities to detect biological agents.

Now, underpinning a lot of these issues is the ability of DHS to continue to work with its partners, and as Deputy Secretary Lute mentioned, DHS has established those relationships. These partnerships need to continue to develop and mature and I think they need in some cases to meet the expectations of those partners, as well. One area is in cyber security, as I mentioned. But there is also a fundamental need to continue to evolve and improve the Department's management processes. The core of why DHS is on our High-Risk List is the need to develop those management infrastructure processes, in the acquisition area in particular, and also the development and testing of technologies before they are deployed, as well as in the financial management area.

I am very pleased. I have had meetings with Deputy Secretary Lute. I have talked to Secretary Napolitano and their team. I know they are committed to addressing these high-risk issues. They have developed a number of plans. We have an ongoing, constructive dialogue to try to be as specific as possible and make recommendations to strengthen these management areas. We look forward to continuing that dialogue as they make improvements going forward.

Finally, I would note that another theme that we have identified is the need for continued risk-based approaches to these areas and also figuring out what works well from what the Department has been doing and what is not working so well. We have had an ongoing dialogue, encouraged by this Committee, on performance measures to judge DHS's performance, and the Department has developed a number of measures and they are preparing a plan to be released shortly to talk about those issues.

But I think it is terribly important as we enter this period of budget austerity and dealing with our deficit and debt issues to really work hard to make sure that we are making the right investments and using risk-based approaches or expanding things that are working well and we are operating as efficiently as possible, because as all of us know, the resources will not be as abundant, likely, in the coming years as they have been to date.

That concludes my opening statement. Ms. Berrick and I would be happy to answer questions that you have about the GAO work. Thank you very much for your time and attention this morning.

Chairman LIEBERMAN. Thank you. Those were two good statements to set the groundwork. We will do 7-minute rounds of questions.

Let me begin with your last point, Mr. Dodaro, and the whole question of management is not too fascinating, really, as it is to discuss individual programs' successes and failures. But just to put it in context, what we really tried to do in creating the Department of Homeland Security was to take a lot of agencies and departments of our Federal Government that touched on homeland security and disaster response and bring them together with the aim of making a whole greater than the sum of the parts, to make sure the dots were all connected, etc. And I think that was a worthy goal and we have achieved a lot on that.

But in doing that, we created a very large Department, over 200,000 Federal employees from more than 22 agencies, and therefore, created a very large management challenge. The Comptroller General mentions two things particularly, and that is contract oversight and new technologies. But to the extent that you can, let me ask you both to comment on the overall management, which is to say what kind of progress have we made in the 8 years of the Department's history to really blend these 22 agencies together, not that they were ever all intended to become homogenized, but they were intended to work together. As someone—I think it was the previous Secretary, maybe it was the current one—said, the aim at DHS is to make sure that every one of the component agencies is speaking the same language in their own dialect, their own accent—not speaking ethnically but speaking in terms of their agency.

So, Mr. Dodaro, how do you evaluate that part of the management record of DHS?

Mr. DODARO. Well, I think, clearly, the intent of having a lot of synergies with that collection of agencies in place has been evolving and taking place. We pointed out in the past, for example, there were difficulties in coordination among many of those agencies, particularly in the law enforcement area, when they were separate entities, and they had some management problems when they were merged into DHS. So that was one of the reasons that we put them on the High-Risk List when they were formed.

So I think that there has been some progress in this area. The framework for that progress has been in a lot of cases that the plans have been developed require the coordination that are laying out and clearly defining roles and responsibilities. This is a really important issue, not just within the Department but across the Federal Government because there are so many players involved. And if you look at many of our recommendations, they go to clarifying roles and responsibilities——

Chairman LIEBERMAN. Right.

Mr. DODARO [continuing]. Writing them down, having written procedures, and working through communication vehicles to work both within the Department and across departments.

So I would say it is a work in progress, but there have been definite improvements. Attention to this area is constantly needed because of the changing threats and the changing capabilities. And after Deputy Secretary Lute responds, I will ask if Ms. Berrick has anything else. I am sure she will add.

Chairman LIEBERMAN. OK.

Mr. DODARO. Thank you.

Chairman LIEBERMAN. Deputy Secretary Lute.

Ms. LUTE. Thanks, Mr. Chairman, and thanks, Mr. Dodaro, for that. I would say the first thing, Mr. Chairman, that we have been able to reflect is the common narrative that now exists across these 22 agencies——

Chairman LIEBERMAN. Right.

Ms. LUTE [continuing]. And over the life of the Department. Everyone has heard of homeland security and people were not always sure what it meant. We are now very sure what it means, in part inspired and helped by the work of this Committee. It means the

effort to build a safe, secure, resilient place where the American way of life can thrive.

What does it take to do that? It requires that we prevent terrorism, that we secure our borders, that we enforce our immigration laws, that we ensure our cyber security, and that we build national resilience. Everyone in homeland security can find themselves in these missions and in this purpose. So in the first instance, narrating out the story that was originally intended these years ago when the Department was first conceived and formed and having all of the agencies relate the work that they have been doing, that they continue to do in the context of those missions and that overarching vision.

What we have had to do over the course of time, again, building on the work of those who have gone before us, is continue to operate. DHS is overwhelmingly an operating agency, every single day. The "building the plane while flying it" metaphor is apt here, and in fact, GAO points that out in its report. It is a huge challenge.

And so the question for us as a Department is how do we add value in this overarching structure in the day-to-day management of those operations? And we have done everything, as Mr. Dodaro mentioned, from improved planning across the range of threats that we face, improving our information, gathering and sharing across the enterprise, and equipping the entire enterprise with the information that it needs. Working on that front, we need to be developing the ability to do risk assessments that address threats, vulnerabilities, and consequences, to mobilize the assets of the Department across agencies when operations require it, as we often do in disaster response, and to work increasingly on those cross-cutting areas, whether it is aviation planning for acquisition, establishing a single point and resource to use for the entire Department across the range of vetting needs that we have, and other areas like this, acquisition improvement and strengthening, which this Committee knows well the work that we have undertaken under the Under Secretary of Management.

So in the three key areas that this Committee has a right to expect the Department can perform in, can we execute our missions, can we run ourselves, and can we account for the resources that have been entrusted to us? In each of these areas, as the GAO report makes clear and the numerous IG reports, as well, the Department has made progress.

Chairman LIEBERMAN. Thank you. Ms. Berrick, do you want to add anything?

Ms. BERRICK. Yes. Thank you, Mr. Chairman. I would say in the area of management, the most progress has absolutely been in the establishment of plans.

Chairman LIEBERMAN. Right.

Ms. BERRICK. For example, if you look at acquisition management, DHS has a pretty rigorous policy in place that governs oversight of acquisition programs. It is very similar in the information technology area. And, in fact, DHS has efforts underway to improve that.

I think there are three primary areas where they need to focus. One is making sure that they have the resources in place to implement those plans. If you look across the range of DHS's plans and

their management areas, they cite available resources as a No. 1 constraint to implementing them.

I think the second area they should focus on is having oversight mechanisms in place to make sure that they are executing those plans as designed. We have identified a number of these areas, and I will just take acquisition management as an example. A number of times DHS has routinely not followed its acquisition guidance. They have not had executive level oversight over major acquisition programs, and have not developed cost estimates in accordance with their own guidance. So they need to have those oversight mechanisms.

And then, finally, I would say it is demonstrating progress and delivering mission capabilities that they can sustain over time. This is where we are getting at these major acquisition programs, making sure that they can field these programs that meet cost, schedule, and performance expectations and have an infrastructure to continue to be able to do that.

Chairman LIEBERMAN. Thanks for that answer. I will make two comments briefly in response. The first is on the resources. I think that is a very important point for management, and particularly since we are in the middle of it right now as we go through the process of trying to get back toward some kind of fiscal balance in our Federal Government and we are squeezing and squeezing. It is a real temptation to take money out of the management accounts of a Department like DHS because the management accounts have inherent advocates for them. Hopefully, we are. In other words, the programs of the Department all have constituencies. The management really does not in that sense. And the danger is that you will gut the management and, of course, the end result will be that the programs will not be run very well. So I think that is up to us, but that is something we have to do.

Senator Collins and I had this conversation once we were some months into the Obama Administration. We were observing together that there was a kind of market test of the coherence of the new Department of Homeland Security because at the beginning of a new Administration, which was the first new Administration since the Department had been created, that would have been the moment for constituent agencies within the Department to have tried a break-out legislatively or with the new Administration. There was only a little bit of a flurry, not widespread and very short-lived, about FEMA coming out of the Department.

So I think that said that both the first two Secretaries and now Secretary Napolitano and yourself have created a coherence to the Department in a fairly short time, at least to the extent that nobody tried to get out. And I do not mean just because they could not stand being in the Department, I mean because a lot of them have big constituencies of their own and a certain amount of political muscle around here. But none of them, either through the Administration or to Congress, tried to break away. And I think it says that for them, the Department is working as an entity, maybe helping them do their job better.

And maybe one thing that happened after 9/11 is that the kind of turf protection that went on before was impossible to defend after an attack like 9/11, and I think perhaps there is an attitude

now that we had better work together, because, God forbid, something happens, we do not want the press or the Congress to come at us and say, "you were just being parochial, not sharing information, or not cooperating with another agency of the Federal Government and that is why this attack occurred."

So, anyway, that is a long story to say that though we have not reached the ultimate destination here, as GAO reminds us, we have come a long way in the right direction. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Dodaro, the GAO has studied DHS extensively, report after report, recommendation after recommendation. So I want to ask you a fundamental question, a question that we are going to be asked as we seek to reauthorize the Department this year, and that is: Has it worked? Has it made us safer as a Nation? Was it a good idea to bring all 22 agencies together in terms of improving our security? What is GAO's assessment and answer to that very fundamental question?

Mr. DODARO. Well, I think we are definitely better prepared as a Nation to address these issues, and to the extent that we are better prepared, we are safer in that regard, although we need to be vigilant, we need to be alert, and we need to evolve to changes.

I think in terms of bringing the 22 agencies together, there are a lot of different organizational models that could have been used. That was one that was chosen. Our focus has been on making sure that model worked as effectively and efficiently as possible. There were synergies to be gained and they are beginning to gel and develop over time, and so the benefits of putting those agencies together are becoming clear, I think.

With regard to the progress, I would say that the Department, in our view, and this is reflected in our report, has made considerable progress in the mission areas. The management areas that underpin some of the developments really need additional work to be implemented properly to help the missions, whether it is developing and acquiring new technology or looking at cost effectiveness issues and measures over time.

So I think I have addressed all parts of your questions, Senator Collins. Those are very good questions. But that is our response.

Senator COLLINS. Thank you.

Deputy Secretary Lute, I want to turn to the management challenges that both the Comptroller General and Ms. Berrick have mentioned today, particularly in the area of procurement. I mentioned in my opening statement that there have been a string of procurement failures. It spans both Administrations. It has cost the taxpayers literally billions of dollars. And equally troubling, it has delayed the deployment of much-needed technology and equipment.

Here is just a partial list. TSA determined that the explosive trace detectors, the puffer machines that we saw for a while at the airport, did not work in a real world environment. They worked fine in the lab but not at the airports. There was the Advanced Spectroscopic Portal, which DNDO moved to deploy before proper testing and evaluation had been completed.

There have been two major consolidated financial data system failures. With the Emerge II System, $52 million was spent before the project was cancelled. The Transformation and Systems Con-

solidation Project was abandoned this year, in May, after multiple protests, a GAO ruling against DHS, and a lot of money spent. This one, in particular, is very frustrating to me because Senator McCaskill and I repeatedly wrote to Secretary Napolitano. We received written personal assurances that the TASC initiative was critical, and it was on track. We were assured of the soundness of the program's lifecycle cost estimates. And, yet, it is abandoned.

The SBInet program was cancelled by the Administration after programmatic failures. Even the Coast Guard, one of my favorite agencies and one that is very well run, had extraordinary problems for a while with its Deepwater Program because of a failed lead system integrator relationship with the government. In July of this year, the DHS IG issued a report that found that the Department had not leveraged its collective buying power across the Department and thus was paying literally billions more than it needed to.

That is not a great record in the area of procurement. So my question to you is what is the Department doing to better define requirements up front, which is one of the major problems, to ensure real world testing and evaluation, and to ensure that we do not have these string of failures continue into the future?

Ms. LUTE. Senator, as you know, and I have testified before this Committee before on certain acquisitions, this has been an area where we have been working diligently to improve our record and our practice. We have cancelled non-performing programs, that is true, and we have had other challenges in our procurement process, but we have addressed them by looking comprehensively at the acquisition process and tailoring a program. We have been planning within that a process that meets the needs of the Department, which largely, although not exclusively, resides in the acquisition of services and important technologies to facilitate our operations at the border and at airports and across the Homeland Security enterprise.

We have worked in three key areas in the area of procurement. First, on requirements. Let me use, for example, aviation requirements. I now chair a committee composed of members across the Department, principally with CBP and with the Coast Guard, to look at our aviation assets and our aviation fleet, leading toward the reestablishment of a Joint Requirements Board so that we can sensibly prioritize what we need in terms of air fleets and seek the air solutions that are not only the most economical, but the most effective operationally, first and foremost.

We have improved the process of cost estimates that has often bedeviled procurements at every stage, not only the acquisition of items in particular, but the sustainability costs which are intrinsic to understanding the life cycle of those acquisitions, as well.

And we have taken a number of steps to strengthen our procurement workforce—you are very familiar with these—including establishing a Department-wide Acquisition Training Program under our head of procurement and enhancing our internship program. We recently had 60 graduates of that program and we are training more. We also are establishing an Acquisition Corps for our senior personnel so that they understand their responsibilities in the acquisition process.

Importantly in this regard, and something I also know that you have great interest in, is the intersection of the operators with the procurers. It makes absolutely no sense to go down a long, tortured path of procurement without having an operator's sensibility introduced every step of the way. Do we know what we need? Are we considering alternatives for what operationally works? And then are we testing it in an operational environment? All these are areas where we have made strong improvements and will continue to do so.

Senator COLLINS. Is this an area, Mr. Dodaro, where the Department has to show more progress and control before GAO will remove the Department from its High-Risk List?

Mr. DODARO. Yes.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Akaka, good morning.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, for holding this important hearing updating us on the progress in implementing the Department of Homeland Security. This is especially significant as we reflect on the last 10 years since the terrible events that led to the Department's creation.

The Subcommittee on Oversight of Government Management, which I chair, has held several hearings on efforts to reform and improve management of DHS which is vital to executing its mission. The Department has made a great deal of progress, but as we have heard from GAO, the important work is not yet finished. Again, Mr. Chairman, thank you for this hearing and I will have a few questions.

Ms. Lute, and I would like to ask Mr. Dodaro as well—as you know, the entire Federal Government, including DHS, has experienced and will continue to face budget reductions. This has caused delays in consolidating DHS's headquarters and forced reductions in the Management Directorate. Please discuss the challenges DHS faces in effectively executing its mission to protect the Nation in this budget environment.

Ms. LUTE. Thank you, Senator. We are all facing those challenges. We have articulated, though, that within the budget guidelines as articulated by the President, the priority for us, of course, are the five mission areas that we see as essential to homeland security.

Preventing another terrorist attack, such as we saw on 9/11, that is job one for us. We do it every day. We will continue to prioritize that within our budgetary guidelines.

Securing our borders, again, we have achieved significant progress in securing our border and we will continue to emphasize that.

Enforcing our immigration laws, conveying immigration benefits appropriately, as well.

Building our cyber capacity is essential. Developing cyber security for the Nation and building the Nation's resilience, as well, to face all risks and hazards.

We will continue to prioritize these. We will also continue to prioritize the integration of the Department and the management of the Department. There are some that—no one on this Committee, I am proud to say—has ever suggested that, somehow, the management is separate and apart from the line or the programmatic functions. We are one Department. The entire Department is operational and we will continue to prioritize our ability to execute our missions to run ourselves and to account for the resources that we are given.

Senator AKAKA. Thank you.

Mr. Dodaro, I would like to hear you on this, as well. This GAO report is based on observations over the past several years at DHS, but in the last year, the Department's budgetary outlook has dramatically changed. Based on your work, are you concerned that budgetary challenges will reverse any of the recent management progress at DHS?

Mr. DODARO. I think it largely depends on how DHS can implement its mission in the most cost effective manner, and I would point out several areas are critical to that. One is in the acquisition area. It is about 40 percent of the Department's budget, and so it is very important that the acquisitions be carried out according to their plans. As Ms. Lute outlined, they have a lot of efforts underway to try to improve acquisition management. I think it is very important. In the IT area, for example, right now, there are 46 projects at a little over $3 billion that are in need of significant management attention, according to their IT Dashboard.

Second, I think they need to use the assessments that they have done on a risk-based approach to make sure that they are integrated into their plans more. They are beginning to do that more and more, but in order to be cost effective, you have to use your risk assessments more effectively.

Third, as I pointed out in my opening statement, the performance measures, what is working, what is not working, is really critical if you are going to target your resources on areas that are in need of greater improvement or to make sure that you are financing things that are producing the right types of results.

And last, their financial management systems are still in need of reform, and if you are going to operate in a cost effective manner, you need good accounting. You need good cost management processes.

So I think all those things can help them deal in a more cost effective manner and it will be critical in this period of budgetary challenges.

Senator AKAKA. Thank you.

Ms. Lute, DHS has committed to empowering the agriculture mission of CBP with the leadership structure and authorities at all levels necessary for success. I am concerned that unless we fully accomplish this important goal, our efforts to safeguard American agriculture will continue to fall short.

In my home State of Hawaii, invasive species have the potential to cause economic and environmental catastrophe there. I plan to introduce a bill to reinforce DHS's efforts to strengthen agricultural inspection.

Will you commit to work with Congress to make sure CBP is fully empowered and held accountable for effective agriculture inspection?

Ms. LUTE. I will, Senator Akaka.

Senator AKAKA. Thank you very much.

Ms. Lute, last year, the Department released its High-Risk Management Strategy, which I think is an important step for DHS to come off the High-Risk List. However, GAO reports that this plan has not been fully implemented. What more needs to be done to implement the High-Risk Strategy and are there any barriers preventing implementation?

Ms. LUTE. Thank you, Senator. We have made getting ourselves off the High-Risk List a priority for us from a management point of view and I am very pleased to say we have been working very closely with Mr. Dodaro, Ms. Berrick, and the team to identify what we actually need to do. GAO has given us a detailed view on what it takes to get off the High-Risk List and we have responded with an equally detailed plan for executing those steps and we have been working very closely together.

So, I think we are on track. We have issued one report on our progress in June of this year. We will issue another in December of this year. And we are going to continue to march along this track until we succeed.

Senator AKAKA. Thank you very much. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Akaka. Senator Pryor, good morning.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Thank you. Thanks for having this hearing today and I appreciate all of our witnesses being here.

Let me start, if I may, with you, Deputy Secretary Lute. According to the GAO, one reason DHS has missed opportunities to optimize performance across its missions is a lack of reliable performance information or assessment of existing information. That concerns me. How has DHS tried to address this problem and what is the Department doing to try to fix that?

Ms. LUTE. It concerns me, as well, Senator, and we have made identifying common sense metrics of progress a priority for us. We have been working, as I mentioned, with GAO across a range of areas to improve our business intelligence processes so that we can have a fact-based understanding of how we are executing and the effect that our operations are having, and this is across the mission areas and across the components within DHS, including very pragmatic metrics for understanding the effectiveness of our emergency response in FEMA, CBP, ICE, CIS, and TSA, as well.

Senator PRYOR. Since you mentioned different parts of your mission there, let me ask about FEMA. What are you doing to improve financial management practices at FEMA?

Ms. LUTE. Administrator Fugate is very committed to this, as am I, and we are looking across the range of operations that FEMA engages with, both on the preparedness side and on the response side. And I chair, for example, a Department-wide task force to look at the Administration of grants, for example, to streamline our

processes, improve accountability, and, frankly, improve the overall performance of the grant program, as well. But across FEMA, the commitment to management is the commitment that we have in the Department for responsive, timely, effective accountability for the resources that have been given to us in the context of effective delivery of effective operations.

Senator PRYOR. And Mr. Dodaro, is GAO comfortable with the progress FEMA is making on its financial management?

Mr. DODARO. We remain concerned about financial management. We look across the Federal Government and there are only four agencies right now that are not able to obtain a clean opinion on their consolidated financial statements, and DHS and DOD are two of the largest ones on that list of four. There have been a couple efforts to try to get an integrated financial management system in place. Most of the problems are in the Coast Guard area and property accountability at TSA.

So I think the Department is trying to get a good plan together in that area. We are going to be evaluating that to see if they make the necessary improvements. But it is one of the critical areas and reasons for why they are on our High-Risk List and so we are going to continue to give them advice on how to move forward and fix the problems.

Senator PRYOR. Let me ask this. DHS is a relatively new department. It seemed to me when it was started a few years ago, that it would have a chance at a clean slate to set all the operations up the way they should be done and not inherit a lot of issues and challenges from the other agencies and offices that existed before that they brought under the umbrella. Was DHS not set up the right way? What is the origin of this problem?

Mr. DODARO. The origin is—I will ask Ms. Berrick to elaborate on this, if she would like—basically, they inherited the 22 agencies. A lot of them had their own definitions and requirements and systems and methods, and so while it presented an opportunity to start fresh, it also presented a challenge because the Department did inherit a lot of the problems and concerns.

Now, we had mentioned early on and our report reflects that they made more progress in the mission areas than in the management area, and we were concerned about management from day one. We put them on the High-Risk List the day they started operations in 2003 and we have always advocated for more management oversight, and eventually the Under Secretary for Management position was created and that position is now filled.

And so I think, Senator, there was an opportunity. In the early days, there was not enough focus on taking advantage of the opportunity, but they also inherited a lot of problems and a lot of challenges and so they are working their way through those still.

Senator PRYOR. Ms. Berrick, do you have a comment?

Ms. BERRICK. Sure. Thank you, Senator. In addition to inheriting legacy problems from the different components, just by the nature that these are disparate systems among the components that are not integrated together is a challenge in and of itself because the systems cannot speak to each other, and at the Department level, senior leadership does not have the ready access to financial information that they otherwise would have with an integrated finan-

cial management system. So I think it is both inheriting some existing problems and also just the fact that these are disparate systems that do not work well together.

Senator PRYOR. And are they actively trying to address those and fix those problems?

Ms. BERRICK. They are trying to do that through the development of an integrated financial management system. They have had a couple of attempts that have not been successful so far, but they are working toward that as their goal.

Senator PRYOR. How much money does it cost to try to integrate a financial system?

Ms. BERRICK. About $52 billion has been devoted thus far.

Senator PRYOR. Ms. Lute.

Ms. LUTE. Senator, the only thing I would add is that is only one component of this. The Department also have made steady progress toward the goal of a clean audit, which is anyone's aspiration. We have gone from over 18 reportable conditions down to six, and we are on track to make even further progress this year and look to do so.

Senator PRYOR. Good. Thank you, Mr. Chairman. That is all I have.

Chairman LIEBERMAN. Thanks, Senator Pryor. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman. To our witnesses, welcome. It is good to see all of you.

I had three questions. The first one dealt with a clean audit. The second one dealt with a clean audit. And the third one dealt with a clean audit. So it sounds like we have mined that field pretty well, plowed that field pretty well.

Let me just ask for the Comptroller General Dodaro, are you encouraged by the progress that is being reported by Deputy Secretary Lute? Should we be encouraged?

Mr. DODARO. Yes. I think, basically, the Department is committed to trying to make progress in this area. As Ms. Lute mentioned, the number of material weaknesses are coming down, but they still have some challenges. Now, they have set some aggressive targets, I believe, to getting an opinion on a consolidated balance sheet for 2011 and to try to get an unqualified opinion or clean opinion by 2014. Those are aggressive targets and those will be the benchmarks as to whether they are successful or not. But they are focused on it. What they really need to continue to focus on is improving their underlying systems, and recover from a couple of efforts that have not resulted in success.

Senator CARPER. And if they are successful in that, it will leave one department as an outlier in this, is that correct?

Mr. DODARO. One major department would be the Department of Defense.

Senator CARPER. I guess as an aside to our colleagues, I had a chance to meet, I think in the early part of August, with Secretary Leon Panetta, who indicated that the idea of waiting until 2017 to reach that goal of audited financials and then maybe hearing from some of those folks that said they were not probably going to be able to make that goal. What he said to me in our conversation—

he may have said the same thing to you—is "I would like to beat that goal" rather than have to slide further. Sometimes it is good to have somebody who was the former Budget Committee Chairman and OMB Director. I mean, he has done it all. But he brings a real commitment to these issues which is very much welcome.

Yesterday, Mr. Dodaro, we had another hearing, as you may know—some of your folks were here—and the issue was the path forward on the Postal Service and how do we help them get back on track. I described the situation as dire but not without hope, and I thought we had a very good hearing.

One of the questions that is before us, and I know it is not the subject of this hearing, but I want to ask while you are here, there is reason to believe that the Postal Service has overpaid its obligation into the Civil Service Retirement System to the tune of $50 billion, maybe as much as $75 billion over time, and overpaid the amount that they owe to the Federal Employee Retirement System by maybe $7 billion or so. We had yesterday one of the witnesses from Segal and Company Auditing, a very nationally renowned company, along with the Hay Group, they have done independent audits to determine what is the validity of the overpayment, has there really been an overpayment. The IG at the Postal Service alleges, and both Segal Company and Hay Group have said, yes, we think there has been an overpayment, anywhere from at least $50 billion to as much as $75 billion.

The Administration is not buying that yet, so we had some discussion there. The head of OPM was here yesterday to talk about that. We asked the witness from GAO if GAO would be willing to come in and take a look at the work that has been done by the two independent auditors to find out if they are valid. We need that kind of direction. If you will, a good housekeeping stamp of approval from GAO, I think, would be very helpful as we try to move and help the Postal Service to dig out of the hole that they are in and return to profitability. So if that is something that you all could help us with, we would be most grateful.

Mr. DODARO. Definitely, Senator. We will be able to do that. We have a Chief Actuary at GAO, as well, that will be integral to figuring out that status. I understand the tasking and the work.

We will deliver that. And as you know, the Postal Service is also on our High-Risk List because of the financial condition situation. So we would be happy to do that.

Senator CARPER. Good. Thanks very much.

Since my first three questions have already been addressed, I will turn to the fourth, and that was cyber security, and it is an issue that the Chairman, Senator Collins, and I have had a whole lot of interest in, and with the help of our staff, I think have done some good work. It is hard to get anything passed around here, but the Administration, I think, has done good work on this front.

But over the last 10 years, Deputy Secretary Lute, as you know, we have witnessed an evolving terrorist threat that has required your Department and other agencies to constantly be thinking about tomorrow's threat. I like to say as an old Naval flight officer, we are pretty good at re-fighting the last war. We are not always very good at looking over the horizon and preparing to fight the next war. But in my view, the next war could very well likely be

on the cyber security front. But nowhere is this more evident than in the world of cyber security, where threats can change almost daily, almost weekly without a whole lot of notice.

GAO has noted much of the good work that your Department has undertaken in this area. GAO has also stated that Homeland Security needs to better secure Internet connections at Federal agencies and more thoroughly share cyber security information with the private sector.

Madam Secretary, I understand that the Department of Homeland Security has a program called Einstein that is helping Federal agencies detect and prevent cyber intrusion. I would ask you, if you will, just to discuss the steps that the Department of Homeland Security is taking to integrate programs like Einstein across the government and what additional authorities, resources, or staffing you need to be more effective. My colleagues here know I like to quote Albert Einstein from time to time, who once said, among other things, "that in adversity lies opportunity." We have plenty of adversity in the world and there is hopefully some opportunity, as well. Maybe this program Einstein can be part of that. But would you proceed.

Ms. LUTE. Thanks very much, Senator. There certainly is opportunity here. This is an area where I have been spending a lot of my time lately, as we have in the Department. We have culled it out as one of the five essential missions of Homeland Security, which is ensuring our cyber security.

What we can all agree is that the status quo in cyber security is not acceptable. There are intrusions. There are threats that we have to address. Cyberspace is an environment right now where offense wins and we have to change that. And our vision is one of distributed security, where we have smart machines and smart users that are supported by intelligent networks that identify threats, hopefully before they occur, that prevent them, and that cultivate a community and a sensibility of cyber hygiene pervasive throughout the United States and, indeed, throughout the Internet, because we are so interconnected.

Einstein specifically is a program that we have, as you know, which is designed to prevent intrusions. We are 84 percent deployed in terms of Einstein II capabilities right now. But the Federal agencies and offices have a number of things that they have to do, as well, to bring their traffic behind Einstein to ensure that they are taking advantage of the deployment of this technology, and we are working with them. In fact, I attended a meeting of the President's Management Council that consists of all the department deputies as the chief operating officers of the departments and spoke to them about what they can do to ensure that their agencies are taking the steps necessary to organize their traffic behind the Einstein protections.

But there are other things to do, as well. What is on your networks? How is information traveling? Who is using your networks? Do they have appropriate levels of access and controls? There is a whole pyramid of efforts—that is perhaps one way to think of it—on top of which sits Einstein. It is only a part of the puzzle necessary to ensure our cyber security.

We are also working very closely with the Department of Defense and with industry. And our, again, vision is to have an environment of distributed security that utilizes all of the assets of this country in protecting ourselves in cyberspace.

Senator CARPER. And if I could, Mr. Chairman, the last part of my question was what additional resources or staffing do you need, what additional authorities do you need in the Department to enable you to be even more effective on this front?

Ms. LUTE. The President's budget that was submitted, Senator, reflects specifics in a number of those areas. We can address this in a stand-alone, if you would like. We have also been working with OMB and there has been a legislative proposal sent to the Hill regarding ways to strengthen our ability to fulfill our cyber security mission.

Senator CARPER. Well, thanks very much. Thanks, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Carper.

We will do a second round, up to 7 minutes apiece, and thanks for hanging in there with us.

I wanted to ask you about a particular part of the Department that the Committee was anxious in the creation of the Department to put in, and that is the science and technology section. Our hope had been—a lot of us on this Committee happened to be on the Armed Services Committee—that we could develop within and for homeland security something like DARPA in the Department of Defense. Over the time of the Department overall, it has appeared to me that the science and technology section has been below what our hopes were. My impression is that it is doing better now, and I wonder if either of you would like to comment on that.

Ms. LUTE. I think I would say at the outset, Senator, that science and technology is a key part of the Department.

Chairman LIEBERMAN. Right.

Ms. LUTE. Our ability to innovate, to make use of end-to-end solutions, not just a particular piece of technology, is a task that we have given to S&T. It has very able leadership with Under Secretary Tara O'Toole, who has integrated into every aspect of our mission performance, working directly with components to ensure that we have a systems approach and are making best use of technology within the context of an overall systems solution.

We also have a very robust cooperation with the other departments, notably the Department of Defense, looking to learn from them on such things as tunnel technology, unmanned sensors, etc., and S&T is critical and important to this and remains a priority for us at the leadership of the Department, certainly for the Secretary.

Chairman LIEBERMAN. Comptroller General Dodaro or Ms. Berrick, have you had any overview of S&T and what is your sense of it now?

Ms. BERRICK. Yes, we do, and I would agree with your characterization that the Department has been slower in making progress in the S&T area. However, I would also agree with the Deputy Secretary that there is a framework in place right now, I think, for the Directorate to be successful. They have put in place additional policies. They have created additional units within S&T to support

efforts like test and evaluation throughout the Department that I think will strengthen the foundation of that Directorate office and enable some successes.

Of the two areas that I would mention related to S&T that I think need continued focus, one is resources. For example, when we did work looking at the test and evaluation function of S&T, we found that they were low in terms of resources and it inhibited the outreach that they could perform with the components in supporting their testing efforts.

And I think the second area that requires focus in S&T is coordination within the Department. We found that sometimes S&T would be pursuing technologies without effectively coordinating with the end users of those technologies to make sure that what they were developing was meeting needs. And a quick example of that is the CAARS program that was being designed to detect shielded nuclear material in cargo and vehicles. DHS ultimately decided to stop that program after learning that S&T was working on developing a system that was not going to fit within primary inspection lanes. So I think that is an example of the internal coordination.

Chairman LIEBERMAN. Yes. Another one is the so-called virtual fence, is it not? My impression is that there was not much interaction with Customs and Border Protection in the development of that.

Ms. BERRICK. We did cite that as a concern that CBP's input on how it was working operationally and challenges that they were facing, were not always fully considered, at least in decisions that were made related to the program.

Chairman LIEBERMAN. I think that is one we all want to keep an eye on because it has tremendous potential both to avoid the kind of problems that Mr. Dodaro cited in terms of new technologies being introduced.

And the second, of course, is more affirmative, which is, as we have seen with DARPA, the ability to leverage Federal money with private innovation and entrepreneurship to create new technologies that will more effectively protect our homeland and also, hopefully, as in DARPA's case, have remarkable spin-offs into commercial applications that will create a lot of economic activity.

Let me ask you, Madam Deputy Secretary, about something a little different, which is the increasing concern that I know the Department and all of us who care about homeland security have had in recent years about homegrown terrorism, self-radicalized people, particularly so-called lone wolves. And I know that the Administration, through Homeland Security Advisor John Brennan, put out a report recently. Senator Collins and I, frankly, were overall—forgive me if I am overstating it—disappointed by the report. We have our continuing concern about the reluctance, refusal of the Administration to use the term "violent Islamist extremism," or something like that, as opposed to "violent extremism." But I want to focus on a different aspect of it.

We also did not see in the report a clear allocation or designation of authority. In other words, who is in charge? And a lot of different departments should be involved in interacting affirmatively with the Muslim American community to gain their assistance in

education and noticing the potential lone wolf behavior, coordinating a lot of the law enforcement education, etc. I know the National Counterterrorism Center, interestingly, has been doing some of that. I cannot say, since that originated in this Committee, too, that we had that kind of function in mind.

The White House, I suppose, has a natural overview which might suggest that it should oversee the response or the prevention of homegrown terrorism, but it has so much that is in the White House now, I wonder whether this is not something that DHS should begin to play a more active role in and I just wanted to give you an opportunity, as now we look back at this decade but forward to the next decade and seeing homegrown terrorism rising as a threat, what you think about DHS's record here and what it might do in the years ahead.

Ms. LUTE. Thank you, Mr. Chairman. We certainly have been playing a very active role. The President's policy that was announced emphasizes three things. First, we need to understand more about what generates this threat and how it promulgates within communities.

Second, we need to engage communities more, break down barriers that isolate them and engage and understand them, create pathways of dialogue and understanding and outreach.

And third, and equally as important if not more so, is strengthen the hand of law enforcement to be able to stop violent extremism in its tracks. Law enforcement prevent crimes all the time quite effectively and we need to equip them with the information and the tools that they need to address this nature of crime, as well.

And so the Department works very closely with the Department of Justice, FBI, NCTC, the White House, and other agencies. We meet regularly on this. We meet as a small group. I meet with my counterparts on exactly this question, about how in each of these areas, in terms of understanding the threat, sharing information, breaking down barriers that isolate communities, and strengthening the hand of law enforcement, what we are doing every day to address this trend.

Chairman LIEBERMAN. To me, those are the right goals. So who would you say is in charge now of that effort on behalf of the Federal Government?

Ms. LUTE. Certainly under the leadership of the President and the White House, this is coming together, but the work is distributed, as so much of the work is in homeland security.

Chairman LIEBERMAN. No, that I understand, but again, there has to be somebody who is in charge to keep driving it. So would you say it is in the National Security Council?

Ms. LUTE. I would say that it is. It is a working system. Again, I meet with my counterparts in the Department of Justice, the FBI, and NCTC regularly on this subject and there is an enormous amount of work going on in each of those strains.

Chairman LIEBERMAN. We will come back to that. I thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I just want to reemphasize what the Chairman just said. The strategy produced by the White House does not clearly assign the responsibility to an individual who we can hold accountable, whose

progress we can measure. And I still do not hear that from you. You keep talking about, well, we work together. There are all these agencies involved. That is not adequate. We need to have a leader of this effort and I hope you will relay that we are continuing to push on that, as well.

I want to switch to some other issues in my remaining time. The recent hurricanes and natural disasters in this country have reminded us of the importance of ensuring that people are notified as quickly as possible when a natural disaster is looming. Early warning can make a huge difference in saving lives and property and that is why I have been working hard on a bill that would strengthen the Nation's public alert and warning system.

I would like to ask your assessment, and GAO may have something to add on this, as well, as far as where are we in using smart technology so that we are not just relying on the crawl on a television screen, the emergency alert that comes across, since many people are not going to have televisions on, but instead we are using phones, we are using social networking sites, and we are using tools that are more likely to reach more people. Deputy Secretary Lute first.

Ms. LUTE. Thank you, Senator. The public alert and warning system now currently reaches about 78 percent of the population. We have a number of initiatives in play particularly aimed at making progress this year, rolling out the Commercial Mobile Alert System, for example, in New York and Washington, DC, and having the first ever national-level test of the Emergency Alert System, as well. So we are absolutely committed to making use of modern technology, social media, to give people accurate and timely information, because we know that in a crisis particularly, information is a commodity and it is essential to having informed individuals and capable communities.

Senator COLLINS. Does GAO have anything to add to that?

Mr. DODARO. We have not looked at this issue, Senator Collins. It is certainly an important issue and I know we are dealing with it ourselves and communicating our own results of our reports, and so it is very important in emergencies. So we would be happy to take a look at this in the future.

Senator COLLINS. Thank you. Deputy Secretary Lute, I want to talk to you about an issue that is related to the homegrown terrorism threat and that is the insider threat. Certainly, the Major Nidal Malik Hasan case was an example of the insider threat. In a report that was released by GAO earlier this year, GAO took a look at the Transportation Worker Identification Credential program that is used for access to our seaports, and its findings were disturbing in terms of protecting us from the insider threat.

First, GAO found that TSA's background checking process is not even designed to detect fraud. In other words, GAO found that it would be easier to obtain a TWIC card with fraudulent documents than a driver's license. That is very disturbing.

Second, GAO criticized the process as not providing an ongoing check. In other words, once a worker receives a TWIC card, he or she has that TWIC card for an indefinite time, even if there is subsequent information or a conviction or something that would cause the TWIC card to be revoked, one would hope.

What steps has DHS taken to remedy these critical flaws in the TWIC program?

Ms. LUTE. Senator, we share the concern about the insider threat and know that it is one that we have to stay constantly vigilant, and this involves not only those of us in the Federal Government, but also, for example, in our critical infrastructure having programs in place in the private sector so that we know who is working in these facilities and that they are trustworthy for the responsibilities that they have been given. TWIC now covers about two million workers and we have run a number of pilots to ensure that we can strengthen the system with respect to not only the technology, but the reliability of the system end to end.

In this regard, the ongoing checks is something that we are looking at department-wide, because, as we have learned, for example, in the case of Abdulmutallab, the 12/25 bombing attempt, that we have to have an ongoing check of visa holders, for example, and of other credential holders. And I chair an interdepartmental examination of a common vetting platform to bring together all of our vetting capabilities and, again, to deploy them in real time to give accurate, full checks, and also working with the agencies to ensure that we have the requirements fully in hand to prevent fraud and other abuses.

Senator COLLINS. In that regard, that reminds me of the Bowling Green, Kentucky, case where two suspects have been arrested, one of whom's fingerprints allegedly were in a database that should have been checked before the individual was granted asylum and admitted to this country. The Chairman and I have written you a letter with a number of detailed questions since the information that was provided at the hearing where we explored this issue proved to be inaccurate. When do you anticipate that the Department will complete its review of how in the world this could have happened, that an individual whose fingerprints were on IEDs used to attack our soldiers in Iraq was granted asylum and allowed to be a resident of this country?

Ms. LUTE. We expect that shortly, Senator. But importantly, we have taken a number of steps to ensure that cannot happen again. We have expanded our engagement of databases, working also closely with DOD to take advantage of the databases of individuals that they hold. And again, this is part of our common vetting examination to strengthen the system overall.

Senator COLLINS. Finally, I want to ask you about the Department's progress in dealing with chemical, biological, radiological, and nuclear threats. This is an issue that we have held several hearings on in the past, that GAO has also examined. And what GAO found echoed the conclusions of our investigations and that is that there was poor cooperation between DHS and the Department of Health and Human Services in assessing the CBRN risk. In particular, it is of great concern that, under the BioWatch program, a threat agent may not be identified until more than a day after its release. What is being done to improve coordination between DHS and HHS in this area, and also when do you anticipate that the next generation, a more sensitive BioWatch system, will be deployed?

Ms. LUTE. Thank you, Senator. Again, here, we think that we make progress continually with the other agencies in this regard. NBIC, for example, does effectively integrate the information for early warning and response on possible attacks or pandemics in the biosphere, as well.

As you know, the work that we have done, for example, on the global nuclear detection architecture is generating work on an implementation plan to further develop our cooperation with other agencies in identifying threats to the homeland and responsibilities for early action to defeat those threats.

So specifically to answer your question, this is a priority for the Department, one that we are making continual progress toward, and we believe that it will substantially reduce the response time inherent in the detection of a dangerous pathogen and alerting appropriate responses.

Senator COLLINS. But when? What is the time table?

Ms. LUTE. I can get back with you, Senator, on the specifics of that, but this is a program that we have in place and it is a priority for the Department.

Senator COLLINS. If the Chairman would indulge me——

Chairman LIEBERMAN. Go ahead.

Senator COLLINS [continuing]. Just one final question on the Kentucky case, which really deserves it. Can you assure us today that the Department has reviewed the files of every Iraqi national who was admitted under that program to ensure that there was proper vetting, including matching fingerprints with databases in possession of the Department of Defense?

Ms. LUTE. It is my understanding that every person admitted under the program has been vetted, Senator. I will confirm that it complies with the question as you have asked it.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins.

I just want to ask one more brief question. It is about the St. Elizabeths campus project. The last time I looked at the statistics, the Department, and we talked about its management and coordination, was spread through 70 buildings and 40 sites in the National Capital Region, and, of course, that is what motivated the plan to coordinate and collect as many of those as we could on the St. Elizabeths campus. If I am not mistaken, the next step would be to bring the 10 operations centers of the Department together there.

So we are in tough budgetary times. The President delayed some of the projects in his budget. The Senate Appropriations Homeland Security Subommittee, I think, has appropriated a third of what the President asked for and the House has cut all the money out for St. Elizabeths. How bad will that be for the improved management of the Department? I would ask you, Deputy Secretary Lute.

And then I do not know whether you have done this or it is even possible, but Mr. Dodaro or Ms. Berrick, is it possible to make a judgment about the cost effectiveness of not building—I do not know whether it is possible to evaluate what costs the Department being spread out adds to its budget, but go ahead, Deputy Secretary Lute.

Ms. LUTE. Senator, as you know, we believe it is important and there is a wisdom in consolidating the Department to reduce the transaction time in engagements, but also to facilitate coordination, dialogue, information sharing, as well. We remain committed to that view that this is an important step in the development and evolution of the Department.

Chairman LIEBERMAN. Anything to add, Mr. Dodaro?

Mr. DODARO. Well, there certainly would be challenges in trying to come up with the exact quantification that you are calling for.

Chairman LIEBERMAN. Yes, I understand.

Mr. DODARO. One of the things that we could do is look at the Department's business case for the consolidation and offer our thoughts on that.

Chairman LIEBERMAN. I would welcome that, if you could.

Mr. DODARO. Sure.

Chairman LIEBERMAN. Thank you. Thanks to the three of you for being here.

Overall, obviously, we have certain almost parental or possessive interest in this Department because we were privileged to be there to help in its creation, so we would like to think it has helped. I do think both the record and the independent evaluations over the years and the summary that you have offered here as we approach the 10th commemoration of 9/11 says that the Department of Homeland Security has made a difference. And again, it is not an accident that we have not had a major attack on us succeed. Do we have more work to do? Of course, we do.

I would also say, and one of you mentioned this, that a different kind of country after 9/11 would have become much more like a police state. I suppose there are people who feel that at different times, somebody's civil liberties were compromised. I think, overall, really, our record is remarkable. I say that also that in a country as big, open, and free as we are—and we want to remain always as open and free as we are—we are never going to achieve 100 percent security.

But we have come a lot more toward that goal, and we should always aspire to the goal, than we were on 9/11, and it is thanks to the leadership of the Department over these two Administrations and the literally hundreds of thousands of men and women who have worked for the Department, working with colleagues in other departments, the Department of Defense, intelligence, NCTC, etc. So it is in a spirit of gratitude and confidence that both GAO and this Committee will continue to push you to get as close to 100 percent secure as we possibly can.

Senator Collins, do you want to add anything?

Senator COLLINS. No, thank you.

Chairman LIEBERMAN. Thanks very much. We will keep the record open for 15 days for any additional questions and answers. Again, thank you.

The hearing is adjourned.

[Whereupon, at 11:41 a.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11: ARE WE SAFER?

TUESDAY, SEPTEMBER 13, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:02 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Levin, Akaka, Carper, Pryor, Collins, Brown, McCain, Johnson, Paul, and Moran.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order.

Good morning and welcome to our distinguished panel of witnesses: Secretary Napolitano, Director Mueller, and the new Director of the National Counterterrorism Center, Matthew Olsen.

This past weekend in ceremonies and vigils across the Nation, we stopped to remember the nearly 3,000 people who were killed 10 years ago in the attacks of September 11, 2001, and to appreciate the acts of heroism and service by countless Americans on that day and every day since to protect our homeland and defeat the violent Islamist extremists who attacked us on 9/11 and drew us into the war that we are in.

The ninth anniversary of 9/11 last year did not get, obviously, the same degree of attention and neither will the 11th anniversary next year, and in some sense, that is why we are here this morning. This annual status of the threat against our homeland hearing with the heads of these three critically important agencies has become a tradition of our Committee. Senator Collins and I wanted very much to hold it after 9/11 to look back a little bit but really to look forward and to make the point that our work in protecting the homeland goes on.

Even though we had fresh warnings that alerted us over the past few days, over this weekend of commemoration, of a specific, credible, although unconfirmed, terrorist plot against the United States, there is already evidence that in a quite natural reaction, the American people are beginning to forget how real the threat of Islamist extremism continues to be.

There was a Gallup Poll taken last year that showed terrorism ranked at the bottom of six voter concerns—understandably probably because of the intensity of the economic concerns that we have today—behind the economy, jobs, government corruption, Federal spending, and health care.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00223 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

And in a very different way last week, a study was published by the Cato Institute calling for the abolition of the Department of Homeland Security, which essentially would return us to where we were pre-9/11.

In some ways, I think we may be the victims of the success that has been achieved in protecting the homeland since there has obviously not been another mass casualty terrorist attack on American soil since 9/11—something, a reality, nobody would have predicted on that day.

Some have taken this lack of another large-scale attack as further evidence, to them anyway, that the U.S. Government exaggerated the danger posed by Islamist extremism and overreacted in the wake of 9/11. I believe this is a profoundly mistaken and ultimately irresponsible conclusion. We have weakened our enemies, and we have protected our homeland, but our enemies are not vanquished, and that is why our vigilance must be constant and not limited to the understandable public attention given to a particular anniversary.

As the Senate Committee on Homeland Security and Governmental Affairs, it is our responsibility to make sure our national focus is not distracted from the threat.

For our witnesses and the tens of thousands of people who work with them, it is their constant responsibility 24–7, 365 days a year, to protect our homeland. So we welcome them to this annual threat hearing and thank them for the service and for all that their respective agencies have had to do with the fact that we have not had another major terrorist attack against our homeland in the past 10 years.

But the violent Islamist extremist ideology that motivated the attacks of 9/11 remains a potent force, though weakened throughout the world, and increasingly, of course, seems to have an effect in the radicalization of homegrown terrorists, including lone wolves.

Today, we have asked our three witnesses to help us answer at least three big questions. One is to take a quick look back, to the extent they want, at what the U.S. Government and their agencies have done since 9/11. Two, of course, the focus of this hearing is to discuss the current threat, the status of the threat of Islamist terrorism to our homeland. And then the third is to discuss what our government currently is doing to counter that threat.

So for me, the question today is not are we safer than we were on 9/11. I think it is self-evidently clear that we are safer. The question is what are we doing and what should we be doing to make sure that this safety continues to be what it is and be greater in the face of the threat that we continue to face.

The 10-year anniversary of 9/11 has passed. The media and public attention will naturally fade. But this Congress and future Congresses, and this Administration and future Administrations, must stay focused on the threat and its ever-evolving tactics until the ideology is truly vanquished and gone.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

The State of Maine became forever linked to the attacks of September 11, 2001, when two of the hijackers, including the ring leader, Mohamed Atta, boarded an early morning flight to Boston at the Portland International Jetport. From Logan Airport, they set in motion the worst terrorist attack in our Nation's history by seizing control of American Airlines Flight 11.

That evening, Members of Congress gathered together on the steps of the Capitol to express unity. A day that had begun in shock and anger ended with unity and resolve. We resolved to ensure that our country had the tools to detect and deter future plots as well as to identify those who would do us harm.

When Chairman Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004, our goal was to create a strong leader to coordinate the 17 separate agencies of the intelligence community and to change their culture from "need to know" to "need to share" so that next time the dots would be connected in time to stop an attack.

The operation that killed Osama bin Laden represented the kind of successful collaboration of intelligence and operations that we envisioned. Information is now being shared more effectively, both across the Federal Government and among Federal agencies and their State, local, and tribal partners.

Just last week, DHS and the FBI announced a "specific, credible but unconfirmed threat" related to the 9/11 anniversary. The Administration is taking this threat seriously, and appropriately so. It has shared information and intelligence with State and local law enforcement officials in the targeted locations and with others across the country.

Thankfully, there was not an incident over the weekend, but we must consider whether this particular threat has truly passed or whether the terrorists have just gone to ground. We must evaluate for how long should we remain on heightened alert.

This threat demonstrates yet again that the terrorists have not abandoned their quest to harm our country and our people. They continue to probe for vulnerabilities.

Much has changed in the past decade. We have vastly improved the sharing of information across agencies at the Federal level and with State and local emergency and law enforcement professionals. America's chemical facilities and seaports were especially vulnerable a decade ago, and we took important steps to safeguard them. In the case of last week's terrorist threat, the decision to publicize the threat put millions of eyes and ears on the lookout for suspicious behavior on the eve of the September 11 commemoration.

Senator Lieberman and I continue to work to expand our "See Something, Say Something" law. The legislation that we have introduced would provide further protection against lawsuits for citizens who report suspicious activity indicating potential terrorist threats.

When it comes to our homeland security, however, we truly are only as strong as our weakest link. As we saw in 2009 with the Christmas Day bomber and Major Hasan's attack later on Fort Hood, when information is not shared and when warning signals are ignored or overlooked, our security is placed at risk.

The TSA has strengthened airline passenger screening. Nevertheless, a young man was recently able to fly cross-country without a valid government-issued ID and with an expired boarding pass that did not even bear his name.

Similarly, the Department of Homeland Security has bolstered the security of America's borders and identification documents, yet two Iraqi refugees with ties to al-Qaeda were arrested in Kentucky for allegedly helping to carry out attacks against our troops. How a known bombmaker, whose fingerprints we have had for years, was able to enter our country on humanitarian grounds remains an unanswered and troubling question. It appears, however, that this case may reflect the kind of lack of imagination that the 9/11 Commission found to be a persistent failure. While the FBI's analysis of IEDs collected in Iraq and Afghanistan has undoubtedly helped U.S. warfighters, the forensic information being collected from these devices should also be used to screen those trying to enter our country, and we must ensure that the FBI has the resources necessary to do that job.

We must ask this question: Are there other Iraqi nationals granted asylum who were involved in attacking our troops? I know that the Administration is reviewing the files of more than 51,000 Iraqis admitted under this refugee program, but it is deeply troubling that we are still awaiting clear answers from the Administration.

Homegrown terrorism is another challenge and evolving threat. This Committee first sounded the alarm about home-based terrorism 5 years ago and has held more than a dozen hearings on this topic.

Over the past 2 years, 31 arrests have been made in homegrown plots by American citizens or legal permanent residents—an enormous increase compared to the previous 7 years dating back to 2001. Yet, the Administration's strategy for countering violent Islamist extremism is insufficient to meet the threat.

We shall never forget those whom we lost on September 11, 2001. As has been noted often, the terrorists only have to get it right once. We have to be right every time or suffer the consequences of an attack. We are surely much safer than we were a decade ago, but we must be relentless in anticipating the changing tactics of terrorists. As the successful decade-long search for Osama bin Laden proved, America's resolve is our most powerful weapon against those who seek to destroy our way of life.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

Secretary Napolitano is our first witness on the panel. Before she testifies, last Friday morning, the Department of Homeland Security held a departmental commemoration of 9/11, and I was able to attend on the plaza outside the Reagan Building here in downtown Washington. And the Department showed a video that had been made by people within the Department about its history, particularly on that day. I thought it was very impressive—for me, moving—and I asked the Secretary if she would bring it today.

So I am sorry not everybody in the room can see. Maybe you can see that screen over there. But at this point, whoever is in charge of the machine, please turn on the video. It is only about 2 or 3 minutes long.

[Video played.]

Chairman LIEBERMAN. I thought that was great. I hope my colleagues on the Committee agree. Really, it is such a powerful statement of unity. I thought it was wonderful to include Secretaries Ridge and Chertoff in it, and all the component division heads. There was a real sense of unity and resolve. So I appreciate it very much.

And with that, please proceed, Secretary Napolitano, with your testimony.

TESTIMONY OF HON. JANET A. NAPOLITANO,[1] SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Thank you, Chairman Lieberman, Senator Collins, and Members of the Committee. I appreciate the opportunity to testify today on the Department of Homeland Security's efforts to keep our Nation safe against ever-evolving threats.

This weekend, our Nation observed the 10th anniversary of 9/11 and honored the nearly 3,000 innocent victims as well as their friends, their colleagues, and their families. We saluted the many first responders and law enforcement officials who responded with such courage and conviction on that tragic day and in the days that followed.

While these past few days remind us that we must remain vigilant and prepared as threats against our country remain, the recent anniversary of 9/11 is also a time to consider the progress that we have made. As Chairman Lieberman noted, America is a stronger and more secure Nation today. We bounced back from the worst attack on our soil and have made progress on every front to better protect ourselves. We have used our experience to become more resilient, not only to terrorist attacks but to threats and disasters of all kinds.

Following 9/11, the Federal Government, including many Members on this Committee, especially Senators Lieberman and Collins, moved quickly to develop a security framework to protect the country from large-scale attacks directed from abroad while enhancing Federal, State, local, and tribal capabilities to prepare for, respond to, and recover from attacks and disasters here at home.

A key element of this new security framework included the creation of the Department of Homeland Security, and over the past 10 years, DHS and its many partners across the Federal Government, across public and private sectors, have strengthened the homeland security enterprise to better mitigate and defend against ever-present and ever-evolving threats.

Perhaps the best way to illustrate the progress we have made is to apply today's security architecture to what existed when the terrorist attacks of 9/11 occurred.

The 9/11 plot, like many terrorist plots, began overseas, which means our security layers must begin there as well. With respect to intelligence, planning for 9/11 began several years before the actual attacks. Osama Bin Laden summoned operatives to Afghanistan to discuss using commercial aircraft as weapons. Since then, we have strengthened the depth and breadth of our intelligence en-

[1] The prepared statement of Secretary Napolitano appears in the Appendix on page 918.

terprise to get the best information possible wherever the operational planning may occur.

With respect to visa security, all of the 9/11 hijackers applied for visas overseas. Today, the DHS Visa Security Program deploys trained special agents to high-risk posts around the world to conduct targeted in-depth reviews of visa applicants before they reach the United States. We have additional layers of security in place through the Department of State's visa checks and pre-departure screening measures. And not only has DHS now reviewed a historic backlog of overstay leads for national security and public safety concerns, but this process has helped put an enhanced biographic exit system on the fast track.

With respect to international information sharing, the hijackers began preparing for the attack while living abroad. Today, 18 countries have joined the United States in agreeing to share information about potential terrorists and criminals through a series of Preventing and Combating Serious Crime Agreements, and more are underway.

After 9/11, the Federal Government discovered that information existed about the hijackers well before and after they came to the United States, but this information had not been coordinated, shared, and analyzed. Since 9/11, the Federal Government, along with its State, local, tribal, and private-sector partners, has made significant improvements to enhance information sharing and analysis.

With respect to targeting, the Federal Government, and DHS in particular, has become more effective at analyzing travel-related data to better understand and anticipate the travel patterns of known or suspected terrorists. This analysis has been essential in identifying, targeting, and interdicting known and suspected terrorists, and prompting additional screening, before these individuals travel to the United States.

We have established 72 fusion centers, which serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information among the Federal, State, local, tribal, territorial, and private-sector partners. Today, the intelligence community is able to identify the common threads that can tie a seemingly minor crime to the larger threat picture, and all but a few of the fusion centers are now connected to the HSDN, which is a secret level, real-time data system sharing data across our country.

Once the 9/11 hijackers made it to the United States, they still required access to aircraft. With respect to flight schools, prior to 9/11, the hijackers enrolled in flight schools and conducted cross-country surveillance flights. Today, the TSA screens all foreign students seeking flight training against terrorist, criminal history, and immigration databases.

With respect to passenger screening, 10 years ago, the 9/11 hijackers were able to purchase tickets and board planes carrying weapons. Today, through the Secure Flight Program, DHS prescreens 100 percent of the 14 million passengers flying weekly to, from, and within the United States against government watch lists.

And Senator Collins, I think I can elaborate, that would have, if it had been deployed, prevented the situation you referred to with the boarding pass.

Moreover, Transportation Security Officers at more than 450 airports now screen all checked and carry-on baggage for explosives, weapons, and other threats using cutting-edge technologies.

And with respect to behavior detection, even though some of the 9/11 hijackers were randomly selected for additional screening and aroused the suspicion of gate agents, they still made it onto a plane. TSA's Behavior Detection Officers today work to identify potentially high-risk passengers who exhibit behaviors that indicate they may be a threat to aviation security and refer them for additional screening.

The last line of defense against threats to aviation security is on the plane itself. With respect to airplane security, today, all commercial aircraft have hardened cockpit doors and Federal Air Marshals are deployed across the aviation system based on risk.

And with respect to emergency communications, limitations in communication and interoperability among air traffic control operators, military personnel, and first responders hindered the response on 9/11. Our Nation has since made significant investments in training and technical assistance to improve emergency communication capabilities.

Each of these layers combined creates a stronger security architecture that did not exist on 9/11 and that has helped keep our Nation, our transportation system, and the American people safe over the past 10 years.

We would not be where we are today without the direct involvement and support of the Congress and particularly this Committee. I want to thank you for your support, your guidance, and your continued oversight.

We continue to engage the broader homeland security enterprise in our Nation's protection. We have made great progress, but more remains to be done. Thank you.

Chairman LIEBERMAN. Thank you, Secretary Napolitano. That was an excellent statement. I particularly appreciate the pre-9/11 comparison to today because it documents in a very tangible way the progress we have made and it backs up a conclusion that I have come to over the years, and it is a painful one, which is that 9/11/01 could have been prevented and should have been prevented and that if it was tried today, it would be prevented, and that is a very important thing to be able to say.

Director Mueller, thanks for being here. Talk about change, though as compared to the Department of Homeland Security, which did not exist on 9/11, the FBI obviously is a venerable American institution, but it has gone through a dramatic transformation in the last 10 years under your leadership to become our domestic counterterrorism agency and really a first-rate one at that, and I appreciate it. Also, we thank you for agreeing to stay on for 2 more years. I suppose I should also thank your saintly wife for allowing you to stay on.

Mr. MUELLER. Most appropriate, yes. Thank you.

Chairman LIEBERMAN. So please proceed with your testimony.

TESTIMONY OF HON. ROBERT S. MUELLER III,[1] DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. MUELLER. Thank you, sir, and good morning, Mr. Chairman, Senator Collins, and Members of the Committee. I thank you for the opportunity to appear here today before you.

As has been pointed out, since September 11, the threat from terrorism has evolved in ways that present new challenges for the FBI and our partners. Today, the threat environment is far more complex and diverse than ever before.

And in response, the FBI has undergone unprecedented transformation over the past 10 years, as you pointed out, Mr. Chairman. We have developed new intelligence capabilities necessary to address terrorist and criminal threats. We have created the administrative and technological structure to meet our mission as a national security agency. And we have made these changes while continuing to safeguard American civil liberties.

Let me begin by focusing on the most serious threats we face and then discuss how the FBI has changed since September 11 to counter these threats.

Al-Qaeda in the Arabian Peninsula and its leader, Anwar al-Awlaki, have shown a commitment not only to attack the United States but also to inspire acts of terrorism from overseas. For the past 2 years, AQAP has undertaken a task directly targeting the homeland. We saw this with a failed attempt to send package bombs to the United States on cargo planes and in the attempted bombing on Christmas Day the year before. And in online media, al-Awlaki and other AQAP leaders have reaffirmed their commitment to this type of attack.

They also continue to emphasize lone actor operations in the West and have sought to radicalize individuals over the Internet to carry out attacks here and in Europe. And despite the recent counterterrorism successes abroad, and there have been many, core al-Qaeda also remains committed to high profile attacks directed at the West. We saw this with the 2009 plot by Najibullah Zazi, a plot to attack the New York subway, and we confirmed this from the materials seized from the raid on Osama bin Laden's compound last spring.

And as you know, we continue to track the current threat streams from al-Qaeda, threat streams that became public last week.

Other groups in the Fatah region of Pakistan, such as TTP, have similarly shown an intent to target the United States. We saw this when TTP claimed responsibility for the Times Square attempted bombing.

And we remain concerned that all these groups encourage radicalized Westerners, particularly U.S. citizens, to travel to the Fatah and East Africa for training with the potential to return to the United States to conduct attacks, and of course, the threat from homegrown violent extremists is among our most serious terrorism threats today.

[1] The prepared statement of Mr. Mueller appears in the Appendix on page 943.

Individuals may be radicalized over the Internet even if they do not receive direct guidance or training from a terrorist group. These individuals may have diverse backgrounds and life experiences as well as differing motives. Increasingly, they may be acting alone, and for these reasons, homegrown violent extremists are harder to detect and to disrupt. And the FBI, along with our partners—NCTC, the Department of Homeland Security and the other law enforcement and intelligence communities—are focused on these threats more than perhaps 8 to 10 years ago.

And of course, the FBI remains concerned about the domestic terrorist threat as well. Economic and political issues could motivate white supremacists or militia extremists to violence. As you know, domestic terrorists can often operate as lone offenders or in small cells, which are difficult to detect.

Overall, the threat environment has evolved significantly since September 11 and is more complex and diverse than ever before, and this requires the Bureau and our partners to change and adapt constantly to address these threats.

As you pointed out, Mr. Chairman, the FBI has undergone unprecedented change in the years since September 11. Today, the FBI is a stronger organization as a result, and we continue to focus on national security threats as our highest priority.

After September 11, the Bureau shifted 2,000 agents from criminal investigations to national security matters. Over the years that followed, we centralized management of counterterrorism and intelligence operations at headquarters to avoid the stovepiping of information.

Structurally, we created the National Security Branch in 2005 to consolidate and integrate the Bureau's overall national security mission and gave senior executives the authority to accelerate the integration of intelligence into our national security operations.

We established the Directorate of Intelligence at headquarters to manage our intelligence programs nationwide. We created Field Intelligence Groups in each of our field offices to prioritize intelligence collection in each of those field offices, and we hired and trained thousands of new intelligence analysts and agents to enhance our intelligence capabilities.

Following September 11, the FBI greatly increased the number of Joint Terrorism Task Forces operating around the Nation. We now have more than 100 of those task forces. These task forces bring together the expertise from our Federal, State, and local partners, and this cooperative effort has led to numerous successes in disrupting terrorist plots and threats since September 11.

After September 11, the FBI also recognized the need to recruit, hire, and train the intelligence analyst cadre necessary to meet the requirements of our national security mission. In 2001, the Bureau had approximately 1,000 intelligence analysts and fewer than 30 supervisory analysts. Today, the Bureau has tripled the number of intelligence analysts to more than 3,000, and we have more than 270 supervisory analysts.

Let me, as an aside, also emphasize the FBI's role in countering cyber attacks—one of the most significant and complex threats facing the Nation. With our intelligence and law enforcement capabilities, the Bureau is positioned to investigate and disrupt cyber in-

trusions, and our need to counter cyber attacks cuts across all of our programs, including counterterrorism, counterintelligence, and the criminal programs.

Beginning in 2007, we worked with our partners to establish the National Cyber Investigative Joint Task Force, which now includes 20 Federal and intelligence community agencies. Through these partnerships, the Bureau has identified, investigated, and prosecuted an unprecedented number of intrusion cases, and these intrusions have impacted our military, other government agencies, the financial and telecommunications sectors, and other critical infrastructure. Addressing this cyber threat will be among the FBI's highest priorities now and in the years to come.

Let me conclude by thanking the Committee for your continued support of the men and women of the FBI and support for our mission as it has evolved. This has been essential to our transformation and our ability to meet today's diverse threats.

Again, as the Secretary said, I would be happy to answer any questions that you might have.

Chairman LIEBERMAN. Thank you very much, Director Mueller. We look forward to the question period with you.

Matthew Olsen, welcome. Obviously, the National Counterterrorism Center is also one of the most significant new entities created in our government, to put it simplistically, to make sure the dots are connected, but obviously, it does much more than that. This is your first appearance before us since your confirmation, and we welcome you.

TESTIMONY OF HON. MATTHEW G. OLSEN,[1] DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. OLSEN. Thank you very much, sir. Chairman Lieberman, Senator Collins, and Members of the Committee, good morning. As I begin, let me thank you for taking the time to meet with me during my confirmation. I appreciate your counsel and support. I am honored that my first hearing as the Director of the National Counterterrorism Center is before the Committee that authored the legislation creating NCTC.

I welcome this opportunity to discuss the evolution of the terrorist threat and our collective efforts to address that threat. I am also very pleased to be joining Secretary Napolitano and Director Mueller this morning, and it is appropriate that we continue to reflect on the day that our Nation suffered the worst terrorist attack in our history.

After a few weeks as the Director of NCTC, I can report that the Center is a national asset. It is comprised of dedicated and talented intelligence professionals representing a wide array of perspectives and experiences.

I am also proud to lead the Center, continuing the work of others—Andrew Liepman, Mike Leiter, Scott Redd, and John Brennan—and my testimony today reflects the thoughtful and rigorous analysis of the expert workforce at NCTC.

[1] The prepared statement of Mr. Olsen appears in the Appendix on page 955.

Today's hearing asks the question, "Ten years after 9/11: Are we safer?" Chairman Lieberman, as you said, the bottom line is we are safer than we were 10 years ago, but al-Qaeda and its allies and its affiliates continue to pose a significant threat.

Thanks to the skill and the hard work of thousands of men and women in the intelligence, homeland security, diplomatic, and law enforcement communities, as well as our men in uniform, we have made significant progress in the fight against terrorism. With the support and guidance of this Committee and Congress, we have built an enduring counterterrorism framework—the framework that includes the establishment of DHS, the transformation of the FBI, and the creation of the National Counterterrorism Center.

Our Nation has placed relentless pressure on al-Qaeda's leadership, denied the group safe haven and resources, and as a result, core al-Qaeda is weakened. But a decade after the September 11 attacks, we remain at war with al-Qaeda. It is a resilient and adaptive adversary, and we continue to face an evolving threat, as Director Mueller mentioned, from its affiliates and adherents.

In the balance of my remarks, I will briefly describe that terrorist threat and then discuss a bit about the role of NCTC and some of the challenges we face.

First, al-Qaeda's core capability to conduct attacks has been significantly diminished. Again, Chairman Lieberman, in your words, it is weakened but not vanquished. The group remains the ideological leader of the global extremist movement. It continues to influence others through propaganda. Al-Qaeda's senior leadership has advanced several unsuccessful smaller-scale Western plots in the past 2 years, and these plots highlight its ability to continue attack preparations while under sustained counterterrorism pressure.

And just this past week, we acted in response to unconfirmed intelligence of a possible threat that the group was planning an attack in the United States. We, thus, remain concerned that al-Qaeda may be plotting to strike against the United States at home or overseas.

Further, since al-Qaeda's relocation to Pakistan, it has encouraged its militant allies to expand their operational agendas to include U.S. and Western targets, both within the region and overseas. For example, Faisal Shahzad's attempted bombing in Times Square, as Director Mueller mentioned, is a stark reminder that al-Qaeda's allies, such as the Pakistani Taliban, continue to threaten U.S. interests in the Afghanistan and Pakistan region.

Second, 10 years after 9/11, we face a much more diverse and diffuse threat from groups affiliated with al-Qaeda. These affiliates have increased the scope of their operations, seeking to strike some U.S. and Western targets both inside and outside of their respective regions.

The single most capable affiliate is al-Qaeda in the Arabian Peninsula. AQAP's recent gains and Yemen's governing challenges increase our concerns about the group's capability to conduct attacks. Further, the group's propaganda efforts are designed to inspire like-minded Western extremists to conduct attacks in their home countries.

AQAP's two attempted attacks against the homeland—the attempted airliner attack in December 2009 and its attempt to down

two U.S.-bound cargo planes in 2010—show that the group is a determined and capable enemy that is able to adjust its tactics.

Third, a key element of the evolution of the terrorist threat since 9/11 is the advent of homegrown violent extremists, as you mentioned, Senator Collins. These individuals are inspired by al-Qaeda's global extremist agenda. Over the past 3 years, we have seen an increase in violent extremist English content online. This has fostered greater cohesion among homegrown violent extremists. Plots disrupted during the past year appear to be unrelated operationally but may share a common cause, rallying independent extremists to attack the homeland.

A key feature of this trend has been the development of a narrative that addresses the unique concerns of U.S.-based extremists. This narrative includes a blend of al-Qaeda inspiration, perceived victimization, and a glorification of homeland plotting. HVEs who independently plan attacks with no direction inside the United States or overseas are difficult to detect and disrupt and could advance plotting with little or no warning.

Now turning to the role of NCTC, as the terrorist threat has evolved over the past decade, so has the government's ability to counter that threat. NCTC has proven to be a vital element of the government-wide effort to counter terrorism.

First, as you know, NCTC has unique responsibility to examine all international terrorism issues, spanning geographic boundaries so that we can analyze intelligence regardless of whether it is collected inside or outside the United States. NCTC has access to the full catalog of reporting, both foreign and domestic, on terrorism issues.

Last year, NCTC created the Pursuit Group to develop tactical leads and pursue terrorism threats. Pursuit Group analysts look for connections among less obvious details to help ensure that terrorist threats are fully examined.

NCTC continues to implement important reforms in the watchlisting process. This includes better processing and sharing of watchlisting information. Our watchlisting experts work closely with NCTC's Pursuit Group, with the FBI, and with the Department of Homeland Security to expedite the sharing of information and to build more complete terrorist identities.

NCTC also conducts strategic operational planning for counterterrorism activities. In this role, NCTC looks beyond individual department and agency missions toward the development of a single unified counterterrorism effort across the Federal Government. We develop plans to help translate high level strategies and policy direction into coordinated activities.

Finally, as this Committee is well aware, the Center continues to be the home to the Interagency Threat Assessment and Coordination Group. This group is led by DHS in partnership with FBI, and it brings together Federal and non-Federal intelligence, law enforcement, and first responder communities to bridge the intelligence information gap between traditional intelligence agencies on the one hand and State, local, tribal, and private-sector partners on the other.

I would like to close today by identifying NCTC's most important resource, and that is our people. As NCTC redoubles its effort to

meet the terrorist threat, our progress depends on maintaining and developing our talented and diverse workforce. We bring together professionals from across the government to focus on a single mission—counterterrorism—and we must strive to work collaboratively, to share information, and to integrate our efforts.

Finally, all of our activities must be consistent with our core values and the protection of privacy and civil liberties. In everything we do, NCTC must retain the trust of the American people as it fulfills its critically important responsibilities.

Chairman Lieberman, Senator Collins, and Members of the Committee, I thank you for the opportunity to testify today. As you know, perfection is no more possible in counterterrorism than it is in any other endeavor, and we will always strive to improve. Your leadership, support, and direction have been invaluable in helping us move forward to carry out our mission and to work with resolve and with unity to protect the Nation. Thank you.

Chairman LIEBERMAN. Thank you, Director Olsen. Thank you very much.

We will go to the questions now. We will start with the first round of 7 minutes for each Senator.

Let me begin by going to the threat stream that alerted everyone in government and the Nation last week as we approached the 10th anniversary weekend. It was described as specific, credible, but unconfirmed or uncorroborated.

Let me ask you first what is the status of our review of that threat now. Do we consider it to be an ongoing threat, Secretary Napolitano or Director Mueller?

Secretary NAPOLITANO. Chairman Lieberman, yes, we consider it an ongoing threat, and we continue to monitor that threat.

Chairman LIEBERMAN. Director Mueller.

Mr. MUELLER. Yes, the threat has not been resolved, and until it is resolved, it is an outstanding threat that we are following up on. Even though September 11 has now passed, we do not believe that necessarily means that we should back down. Consequently, we, the Department of Homeland Security, NCTC, and the intelligence agencies are pursuing that as hard and heavily as we have over the last several days and will continue to do so until it is resolved.

Chairman LIEBERMAN. So it remains, if I hear you correctly, unconfirmed, but again, the intelligence stream was specific and credible enough that you are not prepared to dismiss it.

Mr. MUELLER. No.

Chairman LIEBERMAN. Mr. Olsen, do you want to add anything to that?

Mr. OLSEN. I share the views of Director Mueller and Secretary Napolitano. We are not prepared to say that it has been resolved, and we are continuing to work to analyze it and share information about it.

Mr. MUELLER. I would like to add one thing if I might, Mr. Chairman.

Chairman LIEBERMAN. Go right ahead.

Mr. MUELLER. Since we first had word of that threat, we have conducted hundreds of interviews; we have been pursuing a number of leads. Consequently, as a result of that, we now have been

able to eliminate some aspects where we thought that we ought to be looking in order to determine whether it was indeed a valid threat, but there is still work to be done.

Chairman LIEBERMAN. Well, that is reassuring from my perspective.

I know there were plans already in place—Federal, State and local—to be prepared to defend against another terrorist attack on the 10th anniversary weekend and particularly with regard to homegrown radicals, or lone wolves, and others as well, but I was impressed by the extent to which so many of the assets that our government has now in regard to homeland security and counterterrorism were brought into action on this threat that we really, I think, would not have been able to do 10 years ago.

One of the things that the 9/11 Commission said was that when they asked the question, who is in charge of counterterrorism or a particular response to the terrorist threat, they did not have an answer. So from my perspective, it looked like you were all really working together very well, but I am interested in knowing who was in charge because at some point somebody has to be overseeing all this.

So who would you say was in charge?

Mr. MUELLER. You have on the one hand the intelligence agencies. You have the domestic agencies—operational, DHS, FBI, and the like—all of whom have been through this before any number of times. And the relationships and the organization comes together very quickly, given our history.

But I would say it is the White House and the Office of the National Security Advisor that makes certain that everything has been taken care of generally through the NCTC as the operational arm or the support arm.

But there is no question about the source of the leadership and the coordination, and I think that is why we have been, over the years, effective in terms of coming together, sharing information, understanding our differing roles, and complementing each other to make certain that the job gets done to resolve the particular threats.

Chairman LIEBERMAN. That is very interesting. So the Deputy National Security Advisor, Mr. Brennan, is in charge of counterterrorism, homeland security, acting on behalf of the President, who obviously is in charge, and coordinating all our assets, but the NCTC plays an operational role on his behalf, a support role.

Do you want comment on that, Mr. Olsen?

Mr. OLSEN. Yes, sir. I would say that, as you put it, John Brennan played a coordinating role on behalf of the President in the last few days in response to this threat.

And our role at NCTC is to be the place where information all comes together because some of the information is coming from CIA, some information is coming from FBI, and lots of information is coming from DHS. We play a central clearinghouse role where we take all of that information, analyze it, and then share back out what we are seeing from an analytical standpoint.

Chairman LIEBERMAN. Secretary Napolitano, do you want to add to that? Does this sound right to you?

Secretary NAPOLITANO. That is right, and it is an amazing coordination thing that I have seen, and I do not think it would have been able to be accomplished 10 years ago.

It is ultimately coordinated out of the White House. We all understand how we fit together. Sometimes it is difficult to articulate. You kind of know it when you see it. But it does seem to increase our ability not only to share information among ourselves, but to share information with the country and receive information back. And that also is a difference between now and 10 years ago.

Ten years ago, I was the Attorney General of Arizona, and it was very difficult to get information as to what was going on with the attacks and what decisions were going to be made with respect to air safety, airports, borders, and all the rest. Now that sort of dislocation does not occur.

Chairman LIEBERMAN. Thank you for that.

My time is running out, but I want to ask you, Secretary Napolitano, one additional question. Probably the most visible part of the change in homeland security since 9/11 for most Americans has been the presence of TSA at the airports, and I think they have done a great job. As you know, it is an annoyance to people, but they put up with it.

In testimony before this Committee, Mr. Pistole has indicated that the Department really would like to move away from a one-size-fits-all approach to a more risk-based aviation security strategy. I wanted to ask you what the Department is doing to implement such a risk-based strategy and whether there are moves that will be made soon in that regard.

Secretary NAPOLITANO. Yes. I was fortunate to take Director Mueller's No. 2 and to bring him over to TSA. So thank you very much. I owe you a draft choice to be named later, I think.

But with the respect to TSA, we are moving to a more risk-based approach to screening passengers and trying to streamline procedures for those passengers who are low risk, which enhances our ability to focus on passengers who we either do not know or who are assessed a high risk.

We are piloting several programs to achieve these goals right now. One of them is the expansion of global entry, which is essentially a program that facilitates international travel. It is really a prescreening of a passenger, and we just got our millionth passenger a couple weeks ago. That really facilitates crossing borders.

We also have been piloting programs to deal with children under the age of 12 with respect to not only taking off their shoes but also pat-down procedures, and we hope over the coming weeks and months to be able to begin rolling that out. It does require additional training of all of the thousands of TSA officers, and that is also underway.

We are, obviously, looking at some of the other procedures that passengers need to make in order to streamline their process through the lines. There will always be some unpredictability built into the system, and there will always be random checks, even for groups that we are looking at differently, such as children under the age of 12. But I think the traveling public will begin to see some of these changes in the coming months.

Chairman LIEBERMAN. That is good to hear. So that, in the foreseeable future, if I hear you correctly, we may be moving to a system where children under 12 would not normally be subject to pat-downs and the like.

Secretary NAPOLITANO. Yes. There will be additional training for a different pat-down procedure for them and also, again, allowing them to leave their shoes on.

Chairman LIEBERMAN. Excellent. That is good news. Thank you.

Senator COLLINS. Thank you, Mr. Chairman.

Madam Secretary, I want to go back to the Bowling Green case, which was very troubling to many of us on this Committee. As I look at the overall statistics, DHS interviewed more than 101,000 Iraqi refugee applicants and approved more than 84,000 for resettlement in this country. This is an approval rate that exceeds 80 percent. I was surprised at the scope of this program; 58,810 Iraqi refugees have been resettled and are living here.

Now I know from previous DHS testimony and from my conversations with the Director that there is a review of those who are here to make sure that we have not missed fingerprints or other data or intelligence that would indicate that a mistake was made in granting them the right to resettle in this country. But that leaves 25,625 who have been approved for resettlement but have not yet been resettled in this country.

Is there a hold on that population until they can be more stringently vetted to ensure that we are not letting into this country people who would do us harm?

Secretary NAPOLITANO. Let me, if I might, answer your question in two parts.

First part, with respect to the 58,000 Iraqi refugees who were resettled pursuant to the original resettlement program, they have now all been revetted against all of the DHS and NCTC databases and the Department of Defense's biometric databases. So that work has now been done and focused.

Senator COLLINS. That is completed?

Secretary NAPOLITANO. That is completed.

Moving forward, no one will be resettled without going through the same sort of vetting procedure. Now I do not know whether that equates to a hold, as you say, but I can say that having done the already resettled population, moving forward, they will all be reviewed against those kinds of databases.

Senator COLLINS. Director Mueller, it is reassuring to hear that those 58,000 individuals have been vetted against the existing databases. But in fact, due to a lack of resources and the fact that it is not easy to vet, match, and lift latent fingerprints, do you not have a considerable backlog of fingerprints that have yet to be uploaded into these databases?

Mr. MUELLER. As I think we discussed, there is prioritization in terms of the explosive devices that we look at, and with that prioritization, there is a substantial grouping of devices that have not been looked at. We have taken the precautions of assuring that we maintain the capability of looking at it down the road, in other words, assuring that if there are fingerprints, they can be recaptured down the road. But as you pointed out before, it is a question of resources, and we do have to prioritize.

If we get an indication of a name of a person who there is some question about, we can do that more thorough review by going into this third tier to determine whether that person's fingerprints appear on any IEDs, but it requires a triggering of information in order to go into that backlog.

And it is not just a small grouping, as I think you understand. It is substantial. And so regardless what additional resources we are given, and with more resources we can do more, nonetheless, there would be ultimately a grouping that we just cannot upload for a variety of reasons.

Senator COLLINS. What concerns me is in the case of one of the individuals arrested in Bowling Green, his fingerprints were in those lower priority IED parts, correct?

Mr. MUELLER. Correct, and as I think you understand, we had to go back and identify where he was and do the additional research. And we will do that and have done it. We will continue to do that.

Senator COLLINS. But that depends on your getting a lead or the name of an individual where you can try to map out where that individual was as opposed to DHS being able to run the fingerprints against the complete database, correct?

Mr. MUELLER. Well, they can run the fingerprints against the complete database, but that database will not have that information——

Senator COLLINS. That is my point.

Mr. MUELLER [continuing]. From the third tier that has not been uploaded because of the amounts of devices we have and the necessity to prioritize.

Senator COLLINS. And that third tier, again, happened to be where the fingerprints of the individual from Kentucky were located.

Mr. MUELLER. Yes.

Senator COLLINS. Madam Secretary, I want to talk to you about fusion centers. I have been a supporter of fusion centers. I have visited two of them—one in a large urban area, one in a rural State. And I have seen the information sharing that they do, and I have been impressed.

But my enthusiasm is not shared by everyone. There are individuals on both sides of the aisle who argue that the fusion centers are duplicative of the Joint Terrorism Task Forces. Why do we need them when we already have this multi-agency task force, particularly in a time of budget constraints?

Senator Warner sent you a letter in June on that issue. Senator Coburn's Permanent Subcommittee on Investigations is looking at the effectiveness of fusion centers. And I know that DHS has conducted a study to identify baseline capabilities that every fusion center should have.

Tell me why we need fusion centers.

Secretary NAPOLITANO. Thank you, Senator. I can speak both as a former U.S. Attorney General and a governor as to the utility of the fusion centers.

They do not duplicate the JTTFs. They really complement the JTTFs. They are portals of entry where we can share information—

and as I mentioned in my opening comments, for all but three, we are now connected at the secret level—and get information back.

As Director Olsen and Director Mueller mentioned, one phenomenon that we are dealing with now is the growth of homegrown terrorists and the so-called lone actor or lone wolf. We need more eyes on the ground than the Federal Government itself can supply. The training and ability to share information about tactics and techniques, early trips that should be looked for can be very helpful.

And it is not just sharing information, Senator, that is important with respect to the fusion centers. It is sharing and expanding analytical capability to different levels of government.

So we now have the 72 fusion centers. We have moved our own analysts into the fusion centers so that they can help not only with the gathering and receipt of information but with the analysis of information, which is helpful.

If you look at Zazi, Faisal Shahzad, and Paulin-Ramirez, who was connected with Jihad Jane, in all of those cases, you would see fusion center activity that was very helpful.

And indeed, these past 3 days, with the ongoing threat that has been described to you, fusion centers are active in that as well.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

For the information of my colleagues, Senators will be called in order of arrival as follows: Senators Brown, Carper, Johnson, Pryor, Moran, and McCain.

Senator Brown.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. Thank you, Mr. Chairman.

Mr. Olsen, several of the recent attempted terrorist attacks against the United States have been carried out by, or inspired by, AQAP. How would you assess their threat to the homeland?

Would you put them at the top of the list of threats by terrorist organizations?

And then as a follow-up, is Yemen on its way to becoming another Afghanistan, i.e., a safe haven for AQAP to plot attacks, and do we have a sufficient strategy in place for Yemen?

Mr. OLSEN. Thank you, Senator.

The response to your first question is that AQAP is certainly among our biggest concerns from a counterterrorism perspective. It has shown itself to have both the intent and capability of carrying out attacks against the United States in the homeland. I mentioned the two examples of that—the Abdulmutallab attack of Christmas Day 2009 and then the cargo plane attack in the fall of 2010.

Beyond the actual attempted attacks, one of the biggest concerns we have about AQAP is its propaganda effort. Anwar al-Awlaki, an English speaker, dual U.S. citizen, has through *Inspire* Magazine sought to inspire potentially radicalized Westerners. The actual issues of *Inspire* Magazine have included step-by-step bombmaking instructions.

Senator BROWN. Yes, and it is interesting. That was my next question. How do they actually get away with that? I mean, how

do they get away with putting bombmaking instructions in a magazine, which is disseminated widely, if you can just tell me?

Mr. OLSEN. Well, that information is put out through an online magazine over the Internet, and it is actually information that is——

Senator BROWN. We have no control over anything like that?

Mr. OLSEN. Well, some of that information is not necessarily unique to AQAP. In other words, one of the biggest concerns about the nature of the information is it is quite basic. It is easy to follow. It does not require someone to be particularly sophisticated to follow those instructions.

So in answer to your question, yes, AQAP is at the top of our list or one of the biggest concerns we have.

With regard to whether Yemen is a safe haven, we are very concerned about the ability of the Yemeni government at this point to sustain any strong counterterrorism efforts, given the governance challenges that it faces. So AQAP has had the opportunity to recruit inside Yemen and to plan and plot inside Yemen. We have put extreme pressure on AQ senior leadership. It has been more difficult for us to put that same pressure on AQAP leaders in Yemen.

Senator BROWN. On the *Inspire* Magazine, in particular?

Mr. MUELLER. Well, let me start by saying we are not without tools to address it. But the fact of the matter is that once you upload something on the Internet, it is exceptionally difficult to try to eradicate it. In fact, I would say impossible.

So while we have tools, the likelihood, the possibility of eradicating *Inspire* from the Internet, understanding it is not just the United States but every country around the world, is virtually impossible. And to the extent that we have some capabilities to address that is something we probably ought to talk about in closed session.

Senator BROWN. Madam Secretary, in your testimony, and I have heard you address this many other times, you talk about our Nation's borders and protecting us from illegal entry, especially in Arizona where you are from. I know it is of great concern to Senator McCain and a lot of the other Members from border States. And quite frankly, I could not agree with you more.

In Massachusetts alone, there are several tragic cases of Bay State residents being killed by persons in this country illegally, and then they either flee or are never heard from, but it really has to stop.

The Secure Communities program is something I believe—I do not want to misstate—you are in favor of, you have worked toward, and you would like to see implemented.

How do you deal with States, for example, my State, where you have a governor or others who do not support it? Is there a way to convince them, cajole them, or incentivize them to get with the program, so to speak?

Secretary NAPOLITANO. Well, Senator Brown, I do support Secure Communities. I think it is a key tool in our immigration enforcement efforts to identify those in the country illegally who are also committing other crimes, are fugitives from existing warrants, are multiple illegal entrants, are security concerns. In other words, we

have to be able to find them, and going to the jails and prisons of the country is a logical first place to start.

Senator BROWN. How do you do your job if you do not have the cooperation from the individual States or people in charge? How do you do it?

Secretary NAPOLITANO. Well, there was some initial misinformation about Secure Communities, but the plain fact of the matter is, it is an interoperability agreement between DHS and the FBI so that when someone is booked and his fingerprints are run through the FBI, there is also a connection over to run them against our immigration databases so that ICE can flag an arrestee before he is released back into the community.

It does not require the specific agreement of a State or locality in order to deploy Secure Communities. Now it is helpful when we have cooperation, and so I am using my powers of persuasion to speak with the governors or mayors or other officials who have been troubled by the program.

Senator BROWN. Yes. It just does not really make sense. We are all Americans first, and when we tackle a problem together, we usually prevail. So I am encouraging others that I know back home in Massachusetts and throughout the country to remember we are Americans first and to work together on these very real terrorist threats and concerns.

If someone is arrested and they are here illegally and they are killing people, whether it is through accident or just through basic murder and mayhem, we should be able to get them out and do it with the cooperation of all government entities.

Secretary NAPOLITANO. Secure Communities was begun under my predecessor. We have actually deployed it now throughout the country. I think we have it in 1,200 sites, and we will have it in every jurisdiction by fiscal year 2013.

Senator BROWN. Thank you. Thank you, Mr. Chairman.

Mr. Chairman, can I just ask you a question?

Chairman LIEBERMAN. Of course.

Senator BROWN. Mr. Mueller also pointed out that there are folks who are American citizens, and they are going over there, they are being trained, and they are using their knowledge when they come back.

What is the status of the Terrorist Expatriation Act that you and I and Senator Collins and others filed? Are we going to refile it? Is it something that he would support?

Chairman LIEBERMAN. Yes, I would be happy to refile that bill with you because I think it continues to be a problem.

Senator BROWN. Great. Thank you.

Chairman LIEBERMAN. Thanks, Senator Brown.

I will just mention very briefly in terms of what do you do about extremist material like *Inspire* Magazine or the other things on the Internet, and what Director Mueller said, and other witnesses too, is that there are certain limits on the Federal Government, but what we have discovered in going over this, Senator Brown, is that with some of the major sites—like Google owns YouTube and Blogger, and Facebook is a separate operation, obviously—if individual citizens complain to them about a particular site having vio-

lent material on it, they all have standards. They actually have people whose job it is to review complaints like that.

And on many occasions—let me say that I have at least one staff member who exercises his individual citizen rights when he is not in the office to complain about this material—Google, YouTube, Blogger, Facebook, they take down those jihadist Web sites. It is quite remarkable.

Now of course—it is the glory and the problem of the Internet—they can pop up somewhere else, and then you have to go at it all over again. But there is that ability by individual citizens.

Senator BROWN. Well, as the President encourages people to call us, I would encourage our citizens, if they feel compelled and moved, to contact those entities to do just that.

Chairman LIEBERMAN. Yes, and it is pretty easy to do if you go on those Web sites. Thank you. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman.

To our witnesses, welcome. Secretary Napolitano, nice to see you. Director Mueller, thanks so much for your willingness to sign on for a longer tour of duty. We are grateful for that. And Mr. Olsen, it is nice to see you as well.

My colleagues have heard me tell this story before, but it is worth repeating, and I am going to take this questioning in a little different direction.

About 2 months ago, we had a hearing in the Finance Committee. The subject of the hearing was deficit reduction, and one of the witnesses was Alan Blinder who used to be Vice Chairman of the Federal Reserve when Alan Greenspan was Chairman. And he said in his testimony, unless we are serious about doing something about health care costs in this country—Medicare, Medicaid, and addressing health care costs—we are not going to really get a handle on the deficit.

So anyway, all the witnesses finished their testimony. We were doing the question period, like this, and it came to me, and I said, Mr. Blinder, you said earlier if we do not do anything about health care costs—that is the 800-pound gorilla in the room—then we are really just playing around the edges.

And he said, that is right.

And I said, well, what would be your advice? What should we do?

He teaches now at Princeton. But he said, I am not a health economist, but here is my advice: I would urge you to find out what works. Do more of that.

That is all he said: Find out what works. Do more of that.

And I said, I guess the corollary to that would be find out what does not work and do less of that.

I think the same is true across government as we deal with the budget deficit. We are happy that the deficit is down. It is only going to be $1.3 trillion, I think, by the end of the year, but the red ink is as far as we can see. In everything that we do, we have to look at it through a prism that says is there a way to get a better result for less money, or a better result for the same amount of money.

And I would just ask of you today to talk with us about some of the things that we are doing that are working, where we need to invest a little more money, and maybe some things where we are spending money, frankly, that does not add a whole lot to our security.

Madam Secretary, would you go first? Here is somebody who has had to live with balanced budgets in governing your State.

Secretary NAPOLITANO. Right.

Senator CARPER. You did a pretty good job, as I recall.

Secretary NAPOLITANO. Thank you. Yes, we did have to balance the budget every year.

First of all, I would resist the notion that some redundancy is wasteful. In the areas with which we deal, some redundancy is helpful because there is always the possibility that someone or something will get through one of the many layers of security that we have in place. So you have to evaluate redundancy differently in this arena, I think, than in some others.

Second, we always have to plan for some human error in the universe with which I deal, which is who or what can get into the country, and how do we know who or what is in the country.

So one of the major improvements that we have been able to accomplish over the last several years is to merge more and more databases that are very robust so that we can look at abnormal travel patterns and the like and to share that information. That is the kind of information we can share with the FBI, with the NCTC, when we are pulling the thread of a threat.

So that is an improvement that we want to continue to make more robust and link up, again, as I said before, with the FBI, NCTC, and other agencies around town.

Senator CARPER. All right. Director Mueller.

Mr. MUELLER. I would look at it from two perspectives. First is internally. Every one of us are looking at where we can make savings——

Senator CARPER. Good.

Mr. MUELLER [continuing]. Whether it be contractors or cutting down in a variety of ways that we are going to have to continue to do for the foreseeable future.

More importantly for us is prioritization, and real prioritization. Not everything can be a priority. And for us, it is programs that we have, the particular crimes and threats that we see out there, and prioritizing our efforts to address those threats and assure that as we do that there is a metric for success as opposed to just arrests, indictments, and the like.

Senator CARPER. We are pretty good at measuring process. We are not all that good in government in measuring outcomes.

Mr. MUELLER. And results. So that is from that perspective.

More generally, within the Federal Government, and particularly in our line of work, the ability for information technology to provide us not only the information we need, but to sort through that information and bring out that which we really need is something that we are all undergoing. It is part of having a federated search capability so that you can do searches across a variety of databases, both internally and externally.

And by doing that and developing that information technology capability, we will save a tremendous amount of money, but more particularly, we share the information across our agencies and have the ability for our analysts to do the kind of federated search that does not require them to go into one database, make a search, come out, and do another one. That is one of the keys in my mind to both information sharing of the future but also doing it in a financially responsible way.

Senator CARPER. All right. Thanks. Mr. Olsen, do you want to add anything?

Mr. OLSEN. Yes. First, let me just say that we are, like the rest of the intelligence community, looking for ways to be more efficient in how we are using our resources, but I would make two points.

The first follows up on Director Mueller's point, and that is, at NCTC we are seeking to create what we have called a counterterrorism data layer, which is to take in all of the data that we can from DHS, FBI, and other agencies to be able to take advantage of advances in information technology, to be able to search across that data, exactly as Director Mueller said.

The actual advances in technology make that a way to actually save money, instead of doing searches manually where you log into one system and then log into a separate system, having all that information available so you can search across a variety of databases and make those connections that you would not otherwise be able to make.

The other initiative that I would identify, which I think has no real resource expenditure, is we have set up, as I mentioned in my opening statement, Pursuit Groups, which are analysts looking at the tactical level for connections that might not be obvious and then taking that information, those connections, and handing those off particularly to the FBI and to DHS as leads to follow up on. That is an area where we are focusing particularly in the aftermath of the Christmas Day attack in 2009.

Senator CARPER. Good. Let me just conclude by recalling the words, as we begin a new football season, of Vince Lombardi who used to say, "If you are not keeping score, you are just practicing."

Another way to say that is, what we measure, we manage, and the idea of looking throughout the Federal Government to see what is working well, how can we invest more money there, and what is not, let us invest a little bit less money there.

Secretary Napolitano, there are two departments in the Federal Government that I think are operating without audited financials. One of them is the Department of Defense. Secretary Panetta said to me that he is going to try to get there by 2017; he is going to push his people as hard as he can. And I think that is great, and we want to help him.

Your new Department is making good progress, and I understand this is something you have put a priority on, and I urge you to keep doing that.

Senator McCain and I have been pushing an idea that you had as a tool as governor, a line item veto. I had this tool as governor. We think the President ought to have that tool and just try it for 4 years, a 4-year test drive, fully constitutional. I think everybody sitting in this room except maybe for one person has co-sponsored

that, and we have about 40 co-sponsors, and we are going to push that.

And I call it a 4-year test drive of line item veto authority, and I think that could be part of the solution, not all of it, but in a day that we are looking for silver bullets, it is not a bad silver BB.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Carper. Senator Johnson.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman.

First of all, I really do want to thank you all for your service, and I mean that in all sincerity. You do incredibly important work, and I certainly appreciate the work and effort that you put into your jobs.

I remember watching the debate over whether you should even set up this Department. I think it was a very legitimate debate.

I come from a background in manufacturing where you are always looking for continuous improvement. So my questions really are from that basis. So I do not want anybody taking offense.

Getting ready for this hearing, "Are We Safer," one of the questions I really asked was, are we as safe as we could be based on how much resource we are actually putting toward the problem here within the Department.

So the first thing I was trying to determine is how much money is really wrapped up in the bureaucracy and the overhead of the Department of Homeland Security, and I looked for the 22 agencies that were consolidated. Their budget in 2002 was about $20 billion as best I can come up with. Now we are spending about $56 billion, almost a three-time increase.

Do you know, I mean, do you have in your mind or in your budgeting process, how much really is the Department of Homeland Security bureaucracy versus how much is the expense based on the mission and putting real assets in place?

Secretary NAPOLITANO. It is a difficult question to answer because one of the key criticisms of the Department when it was stood up was that it did not have enough administration so that things like procurement, acquisitions, and planning were not adequately performed. That is, as Senator Carper mentioned, one of the reasons why there was not an audit capability of the Department. We are making great progress on that score.

So you can call that bureaucracy. You can call it management. But the idea is to have as little management as possible to get the maximum out of a very large, complicated department.

So I can go through component by component and say, when the Department was created, we had 7,000 border patrol agents. Now we have 21,000 border patrol agents, and they are in the field.

I can go through and say, when we started the Department, the TSA really did not even exist, and that has almost had to be built from scratch, with the accompanying personnel, training, and technology.

And I would be happy to sit with you and go through that and see where we are.

We are trying to keep the administrative arm as thin as possible, given what we are asked to manage and how we are asked to manage it. But the goal is, as I said earlier, Senator, to do that with as thin a layer of management as possible to enable and empower those in the field to do their jobs.

Senator JOHNSON. One thing I would appreciate, if you could go back and take a look at the head count of the agencies that were consolidated as a basis. Then I could work it up in terms of now you have 230,000 employees in the Department; 63 are in the TSA.

I know in earlier testimony, Director Mueller, we were concerned about how many FBI agents were really devoted to the task. I just want to ask your opinion. I do not want to put you on the spot here. But do you have frustrations in terms of the resources that are devoted to your activities versus what resources are necessarily spent in just department overhead?

Mr. MUELLER. I had one of those consultants come in several years ago to look at our structure. We are very a flat-line structure. We have 56 field offices that really do the work around the country. And persons from the business community were saying that because they all report to one individual basically, you have a real problem in terms of coverage.

They say, well, you are very thin in terms of management, but you are a very matrixed organization. And so, you do not go through the hierarchy. If somebody is doing counterterrorism in the field, they will call the counterterrorism person back at headquarters.

And traditionally, we want more agents on the street, out in the various communities, doing the investigation. What we find from counterterrorism is that I cannot assign the responsibility for protecting the country to a particular office, and we have to integrate the information and manage the cases, not just domestically, but in concert with the CIA, NSA, and others that are looking at the cases internationally, which has required us to build up a capability at headquarters that we did not have before.

That is frustrating. Everybody in my organization would like to be in the field, but in order to be effective, we have had to build a capability to coordinate our actions.

Traditionally, bank robberies or white collar crimes will be in a particular division. In the cyber arena, you can affect persons in all 50 States. You do not know where they are.

In order to address the cyber intrusions, for instance, it takes a headquarters-managed oversight in order to do it. That is working day in and day out with DHS, NSA, CIA, and the other compartments.

We try to stay as flat as we can be, but given the threats, we have had to develop new organizational structures to address them.

Senator JOHNSON. In hindsight, in terms of coordinating that information, would possibly a more efficient model have been utilizing the counterterrorism center for that liaison, for that coordination effort?

Mr. MUELLER. Well, the counterterrorism center is an analytical agent. What we provide is the immediate response to a lead any place in the country. If you have a threat such as we had last week, we have agents following up on aspects of that lead in every

one of the States in the country. And it is the combination of the analytical capability along with the operational ability to pursue that lead, interview people, do wires where appropriate and court orders, to do surveillances around the country, to do the forensics work that provides the intelligence, which is absolutely essential to bring to bear.

NCTC has none of those capabilities. It is an analytical entity.

Senator JOHNSON. Obviously, one of the tasks of the Department is response to a terrorism attack. Now you could take a look at the earthquake here in D.C. as somewhat of a dress rehearsal. I was not here, but I was told that cell phones would not work for hours. It was a mess getting out of town. There was not a real good evacuation plan.

Have you taken a look at that instance and evaluated how prepared were we and did the Department perform the way you would have expected it to?

Secretary NAPOLITANO. Well, yes, we look at all those instances. When you have a disaster that occurs, the private cell phone capability is often overwhelmed in the first instance. Everybody is trying to call out.

A key question I asked was: Well, what about the responders? Were they able to be in touch with each other and to have effective interoperability? And as far as I know, the answer is yes.

Now the second question relates to the evacuation of the Capital Region. We have had that issue with snowstorms. We had it with this recent earthquake.

We have been working. There is a National Capital Region group that involves Virginia, Maryland, the District, and our Department, working with the Office of Personnel Management, quite frankly, in terms of how do you effect an orderly evacuation of the District. You do not have enough road coverage to do it very well, and that is the plain fact of it. But it can be done better, and that group is in ongoing sessions looking at how they can at least improve evacuation procedures, particularly if the Federal Government is going to go into shutdown.

Senator JOHNSON. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Johnson. Senator Moran.

OPENING STATEMENT OF SENATOR MORAN

Senator MORAN. Mr. Chairman, thank you.

I would like to express my appreciation to our three witnesses for their presence here today, but more importantly, for their efforts to make Americans more safe and secure. I express gratitude on behalf of all Kansans for what you do.

Madam Secretary, let me focus on an issue that has received some attention but in my view less than what we normally talk about in safety and security. We are often talking about transportation—airports, railroads, those kinds of things.

There has been this genuine concern. In fact, the Graham-Talent Weapons of Mass Destruction Commission talked about agro-bioscience, the threat that comes from animal disease. Unfortunately, they gave us an F in their report on our preparation for that occurrence.

In my view, a real threat exists in our ability to deter, detect, and quarantine the introduction of any kind of disease into our food supply.

We have a hearing this afternoon on this topic in which one of your officials from your Department will testify, but I would like to know your perspective 10 years later after 9/11. I think in fact slightly before 9/11, the President of Kansas State University, Jon Wefald, testified in front of an emerging threats hearing here in Washington, DC, about this issue. It was not something that a lot of us thought about.

I would like to have you bring me up to date on where you think we are in regard to that threat.

Secretary NAPOLITANO. I think that threat is one of the many evolving threats that we continue to confront. One of the challenges, Senator, that we have been working on these last few years is to actually improve and replace our laboratory and diagnostic capability because one of the problems with these kinds of threats is exactly that. It is diagnostic, it is quarantine, and decisions need to be made on a very rapid basis if one of the sources of our food supply is beginning to be infected.

We have been working with Kansas on the NBAF. One of, quite frankly, the concerns I have is that in the fiscal year 2012 budget—somebody will correct me if I am wrong, I am sure—I think the Department asked for $150 million for fiscal year 2012. The House mark was $75 million. The Senate mark was zero. I hope that can be explored, and perhaps in the conference between the House and the Senate, we can rectify that.

That facility is, I think, necessary for really the next generation, not just for now but also for the future. And we need to always be thinking not only what is happening now but what we could be confronting, indeed, 10 years from now.

Senator MORAN. I certainly appreciate your comments in regard to the scientific aspect of this. In addition, is there any sense across the country of how we are now prepared, or better prepared, or less prepared to respond to the introduction of some contaminate?

Secretary NAPOLITANO. I would say overall we are better prepared. It obviously involves more departments other than just DHS, but there has been a lot of cross-departmental work. Some exercises have been done. Also, importantly, Customs and Border Protection, with respect to inspecting what can come into the country, has done a lot of work in this arena.

Senator MORAN. Thank you very much. Mr. Chairman, thank you very much.

Chairman LIEBERMAN. Thank you, Senator Moran. You are next, Senator McCain.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Thank you, Mr. Chairman.

I thank the witnesses for their service, and Director Mueller, thank you very much for your willingness to continue to serve.

Madam Secretary, are you aware of the Government Accountability Office report of September 12, 2011, addressed to Chairman Levin and me on the subject "Observations on the Costs and Bene-

fits of an Increased Department of Defense Role in Helping to Secure the Southwest Land Border"?

Secretary NAPOLITANO. I am not sure I am familiar with that particular report, Senator.

Senator MCCAIN. Well, I would refer it to you for your reading.

In the report it says, agency officials identified a number of broad issues and concerns surrounding expansion of DOD assistance in securing the Southwest border. Specifically, DOD officials expressed concerns about the absence of a comprehensive strategy for Southwest border security and the resulting challenges to identify and plan a DOD role.

Are you aware of the Department of Defense concerns about the absence of a comprehensive strategy for Southwest border security?

Secretary NAPOLITANO. As I said, I do not know that report, but I have spoken both with Secretary Gates and Secretary Panetta about the fact that we do have a comprehensive border strategy, what it is and what roles DOD can play to assist us there.

Senator MCCAIN. So you disagree with the DOD officials' expressed concerns about the absence of a comprehensive strategy for Southwest border security.

Secretary NAPOLITANO. Vehemently.

Senator MCCAIN. Well, I would be glad to hear about your strategy because I have failed to see one yet, nor have those residents of my State.

Secretary NAPOLITANO. Senator, we have been trying to find a date to brief you over the last several months, and we just have not been able to arrive at one. But I am more than happy to come in and sit down with you again and go through what is happening.

Senator MCCAIN. Madam Secretary, I would be glad to receive that briefing. We have had one meeting, which was highly unsatisfactory, and you might want to broadcast your strategy to the residents of the Southwest who also, certainly the governors and Senators, agree that there is no comprehensive strategy, along with the DOD officials who expressed concern.

I am sure you are familiar, Madam Secretary, with Operation Fast and Furious. Given the high level of information sharing between the departments, were you made aware of the operation while it was underway?

Secretary NAPOLITANO. No.

Senator MCCAIN. Let me be very clear for the record. You were unfamiliar with Operation Fast and Furious while the operation was underway.

Secretary NAPOLITANO. That is accurate.

Senator MCCAIN. While weapons were transported from the Southwest and the State of Arizona to Mexico, obviously, as we know, with serious flaws in the operation, you were not aware of it.

When was the first time you or someone within DHS was made aware of the operation?

Secretary NAPOLITANO. Senator, I would have to go back and check, but it was, I think, around the time of the death of our agent in Southern Arizona.

Senator MCCAIN. And what action did you take at that time, once you were informed?

Secretary NAPOLITANO. Well, first of all, we want to make sure that the investigation into the cause of the death and prosecution was pursued vigorously, and that was being done. I did meet with the FBI agent in charge in Arizona at the time, and I was told that DOJ was referring the entire matter to the Inspector General. So we have reserved judgment until that report comes out.

Senator MCCAIN. When were you made aware that guns, which were allowed to walk during Operation Fast and Furious, were used in the murder of Border Patrol Agent Brian Terry?

Secretary NAPOLITANO. Sometime thereafter. I do not know a specific date, Senator.

Senator MCCAIN. Maybe you could supply that for the record. We would be interested.

Have you come to any conclusions, Director Mueller, as to who was responsible for this operation? You are doing the investigation, right?

Mr. MUELLER. Senator, we are doing the investigation of the killing of the Border Patrol Agent, and that has been pursued. There have been submissions made in court pursuant to that investigation.

The investigation with regard to the approval of the operation itself is being conducted by the Inspector General's Office of the Department of Justice.

Senator MCCAIN. And have you reached any conclusion so far?

Mr. MUELLER. I am not privy to what the Inspector General's investigation has shown at this juncture.

I was concerned as I would be in terms of the extent to which there was FBI involvement, and I have reached the conclusion to believe that there was not FBI involvement in that particular operation.

Senator MCCAIN. So your conclusion is, who was involved?

Mr. MUELLER. Well, I mean, the fact of the matter is it is ATF, which was the principal agency involved.

If you are asking about who was involved beyond ATF and the agents on the ground, or the others in the supervisory line, that is being investigated by the Inspector General's Office, and I am not privy to their findings to date.

Senator MCCAIN. So we leave it all to the Inspector General's Office as to their conclusions. You, as Director, do not have any role.

Mr. MUELLER. Well, we do not have a role in that particular aspect of the investigation. We have a very important role in bringing to justice those persons responsible for the death of the agent.

Senator MCCAIN. But you are awaiting an Inspector General's report.

Secretary NAPOLITANO. No.

Mr. MUELLER. Not on that. We are pursuing that investigation as to who is responsible, what weapons were used in the killing of the Border Patrol Agent, and we are working with the prosecutor to make that——

Senator MCCAIN. And what conclusions have you arrived at?

Mr. MUELLER. I believe that there are submissions made in court in support of—I would have to get back to you on where it is in terms of charging somebody.

Senator MCCAIN. It would be nice for you to get back to me, but we have a dead Border Patrol Agent. We have a situation which at least for a period of time was out of control. It has been now a number of weeks since this happened. And you would be glad to get back to me?

Mr. MUELLER. Well, I do not know the specifics of what charges have been brought in Arizona with regard to that particular shooting.

Senator MCCAIN. Well, can you share with us what information you have?

Mr. MUELLER. We have information relating to individuals who were there. We have individuals identified as a result of interviews we have conducted. We have done the forensics of the scenes. We have identified the weapons. We are pursuing the weapons.

Senator MCCAIN. And when will all of that information be made privy to the American people?

Mr. MUELLER. Well, it is an ongoing criminal investigation. My expectation is that much of that information will be made available in the criminal proceedings that are brought against the individuals responsible for that killing.

Senator MCCAIN. I thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator McCain. Next is Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, for holding this hearing.

I join all Americans across the world in mourning the loss of the thousands who died as a result of the terrorist attacks a decade ago. As we commemorate this solemn anniversary, we must acknowledge the tremendous progress over the past decade to secure our Nation against terrorist attacks.

I want to commend both Administrations' resolve and successful strategy to prevent another attack. We must also commend the men and women who serve bravely in the military, as well as the Federal, State, and local workers in homeland security, law enforcement, intelligence, and other fields who have made essential contributions to combating the terrorist threat.

This anniversary is an opportunity to reflect on how the attacks still affect our lives today. We must remain vigilant so that privacy and civil liberties are not sacrificed in the name of security. As we reaffirm that we will never forget those who died 10 years ago, let us resolve to continue to take steps to ensure that such a tragedy will never happen again and to strengthen the principles upon which our Nation was founded.

The former Chairman of the 9/11 Commission just released a report listing nine of their recommendations that remain unfinished, including the absence of a functioning Privacy and Civil Liberties Oversight Board. In April, I joined Senators Lieberman and Collins in a letter to the President, asking that he nominate a full slate of members so the board could operate.

And I would like to ask these questions to the panel, and if any of you can comment, fine. Otherwise, if you can provide it for the record, that will be fine, too.

What is the status of the board being formed and how are counterterrorism efforts reviewed—and this is the important part—for privacy and civil liberty concerns, given that the board is dormant?

Madam Secretary.

Secretary NAPOLITANO. Senator Akaka, I do not know the status of the board itself. I can say that at the Department, we have a presidentially appointed Privacy Officer who runs a Privacy Office. They are integrated into all of our program planning, particularly with respect to information sharing and how that is done—making sure, for example, that when we enter into MOUs with the NCTC on the exchange of information, we include within those limitations on uses and users, audit, training and also that we, with respect to U.S. persons, put some special limitations on time of retention of certain types of records so that those kinds of privacy concerns we think about before we move forward. They are important to protect.

Mr. MUELLER. Senator, we have three ways.

The first is, we have attorney general guidelines—we have had them for a number of years—that guide our investigative activities.

Second, we do also have an individual responsible for overseeing our particular initiatives from the perspective of impact on privacy and civil liberties.

And third, again, when we have some form of initiative that is being undertaken, we have a panel review of that initiative, which has a person certainly from our legal counsel's office but also from the Department of Justice that oversees that particular undertaking as being reviewed by the panel.

Mr. OLSEN. Senator, I do not know the status of the board, but I would say that at NCTC, we really have what I would consider to be three layers of oversight that consider our activities from a civil liberties and privacy perspective.

First, internally, we have a Civil Liberties and Privacy Officer assigned to NCTC. The sole purpose of his role is to review our activities from that perspective. We also have attorneys within the General Counsel's Office of the DNI who conduct somewhat the same activities with respect to our work.

Second, all of our handling of U.S. person information is done pursuant to attorney general guidelines as Director Mueller made reference to. As well, when we handle information that was obtained under the Foreign Intelligence Surveillance Act, the FISA Court has a role in overseeing that activity.

And then finally, I would mention that we are subject to very robust congressional oversight through the House and Senate Intelligence Committees.

Senator AKAKA. Thank you.

Secretary Napolitano, as you know, the Asia-Pacific Economic Cooperation leaders' meetings will be held in Honolulu, Hawaii, in November. This high profile event has raised concerns that Hawaii could be a target of a terrorist attack. Local residents have also expressed concerns about the Island of Oahu being locked down as a result of security measures.

How are the U.S. Secret Service-led security plans progressing and how will they inform the public about areas to avoid and businesses impacted by security measures?

Secretary NAPOLITANO. Thank you, Senator. The meeting you reference has been designated a National Special Security Event, a meeting for which the Secret Service will provide lead organizational responsibilities, but we will work very closely and are integrated with officials in Hawaii and local law enforcement. They are an integral part of planning and execution in any NSSE event.

As the event gets closer, there will be a public relations plan, for lack of a better phrase, to make the public aware of what areas will be closed down and the like.

One thing I would say to reassure the residents of Oahu is when we do these NSSEs, we are very conscious of the fact that people actually live in these cities and they still need to get to work and school, and so forth. For example, next week, we will have the U.N. General Assembly convene, and we will have many national leaders in New York City, and still New York City will work and people will be able, and have been able, to get to where they need to go for the most part.

So we are very sensitive to that. We acknowledge that. I just use the General Assembly as an example of an event that is perhaps even more complex than the one in Oahu to say that we have some experience here and we will deploy our best efforts in Hawaii.

Senator AKAKA. Thank you. Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka. Senator Paul.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Thank you, and thank you to the panel for coming today and these presentations.

Secretary Napolitano, we have admitted about 70,000 Iraqis over the past 3 years. Two of which I think Senator Collins brought up earlier were arrested recently in Bowling Green on accusations of conspiring to be involved with terrorism.

I can kind of understand that after we lost the war in Vietnam, the communists took over and people who sided with us or fought with us would be executed. But my understanding is we won the war in Iraq, and we are admitting 70,000 Iraqis when we won the war and there is a democracy over there.

What reason do we have to be admitting so many, and is the policy of the Administration to continue to admit so many, and is it not a danger to our country and overwhelming us with numbers of folks who have to be screened and apparently sometimes are not screened properly?

Secretary NAPOLITANO. Well, Senator, as I explained earlier, we have now gone back and rescreened the Iraqi population who were admitted as refugees against all of the DHS databases, the NCTC databases, and the Department of Defense biometric databases, and for any future refugees, we will continue to do the same.

And then, if there are particular hits or particular concerns on individuals, we refer them sometimes to the FBI to do further investigation or checking.

Senator PAUL. Does the Administration have a position though on admitting so many people and continuing to admit so many people from Iraq?

Secretary NAPOLITANO. Well, the refugee program was begun under the prior Administration, Senator, and many of the individuals who have been rechecked were admitted then.

With respect to the current time, if people qualify for refugee status under the law, they will be permitted to come in, but they will be vetted.

Senator PAUL. I understand the number though is determined by the Administration. Your Administration determines the number, and if you decided you wanted to have 3,000 next year, my understanding is under the law you could.

Secretary NAPOLITANO. My understanding, Senator, is that is being done primarily by the State Department and a number of considerations are taken into account.

Senator PAUL. The argument is that it is unsafe in Iraq, but I think it is sort of an insult to our soldiers who are over there to say that it is unsafe. Our soldiers are still there protecting their country, but it is so unsafe that Iraqis get to leave and come over here.

I guess really to add insult to injury is not only do we bring them over here, but both of these people who are accused of terrorism in our country were living in government housing and on food stamps.

Now in the 1996 Welfare Reform Act, we said that if you come here legally through immigration, you would not qualify for welfare. I think we should change that.

Does the Administration have a position on refugee status and whether or not they should be coming here and immediately put on welfare?

Secretary NAPOLITANO. Senator, I cannot answer that question right now. I will get back to you.

Senator PAUL. Bowling Green seems to have been in the news—Bowling Green, Kentucky, where I am from. We had a little girl from Bowling Green, who was on Good Morning America, who had a TSA agent do an invasive search inside of her clothing, inside of her pants. We had an 8-month-old who had his diaper inspected. Then we had a 95-year-old who had his diaper taken off and inspected and stayed, I presume, for hours waiting to get through the TSA.

Earlier this year, TSA Administrator Pistole said that we need to do these invasive searches, and he said that we may slow down or we may not do them as much.

But then he sent me a letter and said that we absolutely have to because an 8-year-old in Kandahar exploded a bomb.

To me, I think that shows a bit of naivete to think that somehow there is a similarity between an 8-year-old in Kandahar and an 8-year-old in Bowling Green, Kentucky. I mean, the only similarity is their age, and I would not consider age to be a risk factor. If anything, age might argue against a risk. But to say that she is the same age as someone who exploded a bomb in Kandahar—I mean, we have to bring some sense to what we are doing in this country.

After 10 years, why do we not have a frequent flyer program?

A big bulk of those traveling are traveling two to three times a week, and yet, we treat everybody equally as a terror suspect. In doing so, we take away time that could be spent on those who would be.

I would have a frequent flyer program. I would have it in a month, and I would take half of the TSA agents, and I would have them looking at the manifests of those flying from foreign countries. I would want to know who is on every flight.

I do not know how far in advance we are doing this, or if we are doing it, I would like to know a month in advance.

I would make strict rules on those flying internationally. I think that is the biggest risk.

With those 70,000 people coming from Iraq, we say that we are going to vet them, but we missed fingerprints that they had on an IED. Even if we do things perfectly, the haystack is too big.

Think of our army. We have people about once every couple of months in Iraq or Afghanistan who we admit into the Army to help us. They are supposedly our allies, and they turn around and shoot us. It is hard to vet these people.

This was an extraordinary circumstance that we had a fingerprint and we missed it, but most of the time they could be completely lying to us as they go through the vetting process. We bring them here, put them on government welfare, and then they are here to attack us.

We have enough problems in our country. We have a lot of poverty in our country. We do not need to be admitting the world's poverty problems, and I think the Administration needs to take a position to lessen the numbers of people coming in from Iraq.

You need to take a position and move forward on a frequent flyer program, and we need to not just be told there is some day going to be risk assessment. We need to start doing risk assessment and paying attention to the people who could attack us, and not wasting and diverting our time and resources and insulting the dignity of those who are traveling.

Secretary NAPOLITANO. If I may, Mr. Chairman, I will simply say with respect to the movement to a risk-assessed based strategy in the TSA, that is exactly what we are doing. And as I said earlier in the hearing, we will be rolling out slowly because you have to train agents as you do this. We move almost 1.8 million passengers a day, and we always have to have a certain amount of randomness and unpredictability in the system because the minute you say an entire group is exempt from screening, they can be exploited as a possibility.

But your point about travelers who are low risk is something that we accept. We are moving to expand the global entry, which is for international travelers. We just passed our 1 millionth traveler. We are moving to expand that.

We are moving to loosen restrictions on children under the age of 12 and also to amend the pat-down procedures that are used.

So these improvements are underway, but I would caution, Senator, that when you say do it in a month, we need to move on a deliberate pace but a careful pace. Our adversaries are very determined, and they are very determined with respect to the aviation system. We want to make sure that we do it right.

Senator PAUL. One quick follow-up to that. Really, I agree with you. It is probably not that smart to say absolutely that we are never going to search anyone under 12 years old. But for goodness sake, could we not make a difference between an 8-year-old from Bowling Green and an 8-year-old from Kandahar?

I do not mind if someone is coming from Pakistan or Afghanistan next week, that you spend a little more time, but we need to understand and use more common sense with what we do. And it really would, in practical purpose, mean that probably 99 percent of kids under 12 would not be patted down, and that would be a lot better for most of us who are insulted by what they are doing now.

Chairman LIEBERMAN. Thanks, Senator Paul. Thank you. Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you very much, Mr. Chairman. Sorry that I could not be here for most of this because I was chairing, as you know and Senator Collins knows, the Armed Services Committee hearing on the confirmation of Ash Carter.

Let me welcome you all. I join my colleagues in doing that.

Director Olsen, let me start with you. I think you note in your prepared testimony that the homegrown violent extremist activity remains elevated with U.S.-based extremists taking inspiration and instruction from al-Qaeda's global efforts in a wide range of its English language propaganda. Part of that propaganda was a recent online video released by an American-born confirmed al-Qaeda operative in which he urges al-Qaeda followers and sympathizers to exploit U.S. gun laws and to purchase firearms.

Now, under current gun laws, individuals are allowed to purchase a firearm without an FBI background check if they are buying from a private seller, such as those at gun shows. Does that loophole make it easier, in your judgment, for homegrown extremists to purchase firearms for use in a terror attack?

Mr. OLSEN. Senator, I have not looked at the gun laws and after 4 weeks in my position would be reluctant to comment on that.

Senator LEVIN. Will you comment on that and get us a report?

Mr. OLSEN. Yes, sir.

MR. OLSEN'S RESPONSE TO SENATOR LEVIN'S QUESTION

Response: As Senator Levin points out, individuals who purchase firearms from federally licensed firearms dealers are subject to background checks. Individuals who purchase firearms from private sellers are not subject to FBI background checks. Federal law makes it unlawful for certain categories of persons, such as convicted felons, to transport, possess, or receive any firearm or ammunition. *See* 18 U.S.C. § 922. It is my understanding that the FBI uses the National Instant Criminal Background Check System (NICS) to determine whether individuals seeking to purchase firearms from federally licensed firearms dealers are eligible to make such purchases.

Senator LEVIN. Thank you. Director Mueller.

Mr. MUELLER. Yes.

Senator LEVIN. And with that FBI background check of individuals purchasing a firearm from private individuals, in your judgment, would that help reduce the threat to us from U.S.-based violent extremists?

Mr. MUELLER. I would have to put it like this: A background check is important in identifying those persons who have some reason for being in the databases, and enhanced coverage of the purchase of weapons would give us a greater ability to identify persons who should not have weapons and prevent them from getting weapons.

Senator LEVIN. That would include the purchase from private sellers such as at gun shows?

Mr. MUELLER. Yes.

Senator LEVIN. Thank you.

Fifty States now form nearly 2 million new corporations each year without knowing who really owns them. The failure to collect ownership information—the actual owners, so-called beneficial owners—invites wrongdoers to misuse U.S. companies for terrorism, money-laundering, tax evasion, and other crimes. It is a subject this Committee has been examining now for some years.

In August, Senator Grassley and I introduced S. 1483, the Incorporation and Transparency in Law Enforcement Assistance Act that would require disclosure of beneficial ownership information in the company formation process.

At that time, the Treasury Department was very supportive and announced the following: "The bill would substantially advance the Administration's fundamental interest in ensuring the availability of meaningful beneficial ownership information about companies created in the United States."

And they went on: "Such legislation is critical to the Administration's objective of protecting the global financial system and strategic markets from abuse."

So we want to first of all thank the Treasury Department for that support, and we are wondering, Secretary Napolitano, whether or not the Department of Homeland Security takes the same supportive position that we need to know for law enforcement purposes, just for law enforcement purposes, who the beneficial owners of the corporations are in order to prevent terrorists and other malfeasers from misusing shell corporations to launder money or for other nefarious purposes.

Secretary NAPOLITANO. Yes, we support it.

Senator LEVIN. I would hope, Mr. Chairman, that we can take up this bill again. I know you have had it on the agenda a couple times, and it has, for various reasons, been on and off our markup.

But I think it is important that we have the testimony from law enforcement here this morning that we need to do what other countries do, by the way. We go after these tax havens for allowing their jurisdictions to be used to avoid taxes from being paid, but one of the things they do at least is they get the beneficial owners of corporations on record so that they know who actually owns the shell corporations, at least in many cases.

And I would hope that, again, we would be able to take that up, and the support of the Treasury Department and the Department of Homeland Security is very helpful. I just wanted to get that on the record for us.

On the Northern border, the GAO in February reported that there are serious security threats to the Northern border and that the risk of terrorist activity is high. It said that DHS reports—now

this is the GAO saying that the DHS reports—that the terrorist threat on the Northern border is higher than on the Southern border, given the large, expansive area with limited law enforcement coverage. That was on page one of that report.

However, even with that high risk of terrorist and other illegal activity on the border, the Border Patrol reports that "only 32 of nearly 4,000 Northern border miles in fiscal year 2010 had reached an acceptable level of security."

I am wondering if you would tell us here today or for the record, Secretary Napolitano, whether that number of Northern border miles has increased.

Secretary NAPOLITANO. I believe it has, and as we have discussed in other contexts, that use of the phase operational control is a term of art.

We have a Northern border strategy. It had to be cleared by OMB. It now has been completed, but we want to update it with the full fiscal year's statistics prior to publishing. It will be published shortly.

The other change I think that is very significant is what is called the Beyond the Border strategy that we now have with Canada, which is a law enforcement information sharing perimeter-oriented strategy that really did not exist 2 years ago when I think a lot of that report was probably researched. That is going to be of enormous importance because it takes pressure off of the physical U.S.-Canadian border and allows us to expand the border outward.

Senator LEVIN. If you could, in your own words, get us the number of miles of border that have an acceptable level of security. I do not mean now. Get it to us for the record, if you would.

Very quickly, if I could, Mr. Chairman, I know my time is up, but I just have one more question and then I have a thank you.

The Urban Areas Security Initiative has a very complex funding allocation formula, and one of the questions is whether or not a location is on an international waterway. For reasons which are totally incomprehensible, Detroit is not listed as being on an international waterway when it is. The Detroit River is an international waterway between the United States and Canada, and not only that, it has more commerce crossing that river at Detroit than any other place probably in the world, much less in the country, in terms of commerce crossing that bridge particularly in Detroit.

Will you take a look at that, Madam Secretary, that issue of whether or not Detroit is on an international waterway? Find out for us why the City of Detroit is not listed because it makes a difference in terms of allocation of resources. So will you take a look at that?

Secretary NAPOLITANO. Yes, I will drill down on that for you, Senator Levin.

Senator LEVIN. Finally, a thank you. Two days ago we remembered 9/11. And following 9/11, there was a small group of people in Detroit representing the Arab-American community and representing law enforcement that came together and formed a group called BRIDGES.

And there has been a really strong connection between the law enforcement community under the leadership of the U.S. Attorney in Detroit, but including also elements of the Homeland Security

Department, so that the communication is far better. The trust is far better. They work shoulder to shoulder now against violence and hatred. It is an important group because if you have the support of community, whatever community it is, working with law enforcement, it is a great source of American security.

And that kind of support in the Arab-American community, in the Muslim-American community is reflected in that group where law enforcement—Federal law enforcement and State and local law enforcement—are represented for frequent meetings. They also memorialized their anniversary the other day with their annual dinner.

And it is a very reassuring thing to see law enforcement in our communities, period, whatever the community is, working so closely together. That is where security is really enhanced. It is not just the typical law enforcement security, which is important—protecting borders and doing other things—but it is also having the support of the people in our neighborhoods, in our communities working shoulder to shoulder with law enforcement.

I just want to commend you both. The FBI is actively involved in that. The Justice Department, U.S. Attorney, and also your elements of DHS are very much involved. And it was kind of heartwarming to see that, and we all feel a lot more secure when that is true. Thank you.

Thank you. I am sorry I went over.

Chairman LIEBERMAN. No, thank you. I join you in that thank you. The Bureau actually was out there right after 9/11, and that probably surprised a lot of people, in outreaching to the Muslim-American community, and it continues to do that. We appreciate that.

Senator Collins and I would like to ask just one or two more questions. You are a very steadfast, resilient group, and I am sure that you have faced worse challenges than the two of us, and just for a few minutes more.

I want to ask you a wrap-up question. We have had a lot of good testimony, good discussion. Of course, I feel very positively about what we have accomplished over the last 10 years. Looking to the next year, let me know what your top one or two priorities are of what is not done to your satisfaction yet in terms of your Department, your Bureau, and your Center.

Secretary NAPOLITANO. Mr. Chairman, our Department has so many elements to it, but I think over the next year, we will continue to improve and expand information sharing and analytic capability with the FBI, NCTC, and other agencies within the Department and outside the Capital Area to the rest of the country.

I believe that cybersecurity will be an increasing area of focus for us as we deal with, as Director Mueller said, really that emergent threat in the cyber world.

I think we will see over the next year a movement toward a more risk-based screening process for passengers, particularly in the air environment.

And last, we want to move toward, we call it—and you heard it in the video that you began the hearing with—one DHS. We are still in the building process, the knitting together processes in-

volved with putting 22 agencies together, and I think we will see even more progress in the year ahead.

Chairman LIEBERMAN. All right. You have a busy year ahead of you. Director Mueller.

Mr. MUELLER. First would be the federated searches capability, both internally and externally, so that while we have to keep, for a variety of reasons, different database structures, there has to be the ability to pull information very easily from those databases.

Chairman LIEBERMAN. Give us a little background for people listening.

Mr. MUELLER. If we have information off a FISA intercept, there are minimization procedures, or procedures about to whom that information can be disseminated——

Chairman LIEBERMAN. Right.

Mr. MUELLER [continuing]. Which requires us to keep it in a separate database. But what you want to do is give the analysts the ability to understand if there is anything in that database on a particular individual, email address, or the like.

Chairman LIEBERMAN. Right.

Mr. MUELLER. While for a variety of reasons we have to keep separate databases, whether it be from security or from statutory direction, there has to be the ability to do the federated searches across those databases, both internally as well as externally, which is where NCTC is putting a great deal of its effort.

So we all have to get our own houses in order in order to be the platform for the government as a whole to be able to do this kind of search capability.

Chairman LIEBERMAN. Do you need statutory changes to do that?

Mr. MUELLER. It would be difficult, if you take the FISA statute, for instance.

Chairman LIEBERMAN. Yes.

Mr. MUELLER. We have just gone through the update of the PATRIOT Act, and I am not certain it is something that would easily get through. So while conceivably you could do it, it is unlikely to happen very shortly, and consequently, we have to utilize technology.

Second, as pointed out earlier, is the cyber arena. Adjusting our organizations to address the cyber threat in new ways that will make us more effective as a united entity is going to be a huge issue.

Third, is the necessity for assuring that new mechanisms of communication that are being developed daily by the new entrepreneurial information technology capabilities by various companies—I do not want to necessarily name them here—but it is not just the communications carriers that carry communications now. It is Google, Facebook, all of them.

Chairman LIEBERMAN. Right.

Mr. MUELLER. And the necessity of assuring that in response to a court order giving us the right to obtain those communications, there is the capability of those persons or those entities to respond to those court orders is something that I will be addressing. We cannot afford, as we say, to go dark.

The last thing I would say very quickly is with enhanced information technology comes additional administrative burdens. One of

the challenges we have is to make certain that our agents or people are spending their time on the substance——

Chairman LIEBERMAN. Right.

Mr. MUELLER [continuing]. And removing some of the administrative burdens and obstacles to getting out there and doing the work that we want to pay them to do. That, for us, is an issue that we continuously fight.

Chairman LIEBERMAN. So it is a substantive list. On that third one, about gaining access to information from the unconventional, the new communications media, that might require legislation?

Mr. MUELLER. I think it will. I think you may see some suggestion with regard to legislation. And I would say most of the companies are very patriotic and working on capabilities, but we have to make certain that they have the capability to respond to the court orders.

Chairman LIEBERMAN. Right, because a lot of times those recipients of court orders want the statute to make clear their obligations.

Mr. MUELLER. True.

Chairman LIEBERMAN. Mr. Olsen.

Mr. OLSEN. Thank you, Mr. Chairman.

Picking up on the theme of information sharing, it is similar at NCTC. As you both know very well, the founding principle of NCTC was to break down the silos of information and provide a place where information from the CIA, DHS, the FBI, and NSA could be brought together. We have made significant progress in doing that, largely through bringing people together in one place from each of those organizations.

I think the next step in that process is to have that information. We have much of it but to continue to gather that information, ingest it, have it available at NCTC where we then can do exactly what Director Mueller talked about at NCTC—search across databases, not have an analyst go to one database, go to another database, and go to a third, but be able to find the connections that are so elusive by being able to search seamlessly across all those databases. So that is one, and that is a significant priority for us.

Second, I mentioned the Pursuit Group. I think that there is a lot of potential there. This was something started in 2010 to fill a gap by looking for less obvious connections among pieces of information, among people, and then to be able to tip those leads off to the operational entities that can follow up, whether that is CIA, FBI, or DHS. I think there is a lot of potential there, and I am going to continue to focus on that.

And third is an area I know that is of significance to both of you, and that is countering violent extremism. This is an area where NCTC has played a vital role, and I think we will play an increasingly important role in the next year in particular as we do a couple of things, but the one I will highlight right now is to develop the implementation plan for the Administration's new framework, a strategy for countering violent extremism.

We have done a number of things on the intelligence side and on the operational planning side to prepare law enforcement to understand the radicalization process, to help communities understand where to look for threats within their neighborhoods and their com-

munities, but there is a significant amount of work to do in this area, and I think NCTC is going to play an important role.

Chairman LIEBERMAN. We agree. As you may know, Senator Collins and I just sent a letter to Mr. Brennan, expressing disappointment with a lot of that report, and a lot of the disappointment had to do with the lack of detail, a lack of clarity, at least as we read it, about who was in charge but also what is going to happen.

Insofar as you are going to put some flesh on the bones, or whatever the metaphor is, clarify that urgently, that would be very important.

I thank all three of you. It is interesting how much cyber comes up. And also, these remarkable instruments of data analysis retention, which have helped us enormously, just were in play in the last week with the latest threat stream. But we can yet do better at that, as you have all said. Thank you.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Olsen, let me take up where you just left off because I was going to talk to you about who is the lead for countering violent extremism.

I know that the White House is the lead for policy and put out what is in our view a disappointingly sketchy strategy. But is the NCTC going to be the operational lead for implementation?

Mr. OLSEN. We will not be the lead for the operational implementation. The National Security Staff and the National Security Council at the White House has the lead for developing the policy. And we at NCTC play a role and will be front and center in developing the implementation plan, putting the flesh on the bones for that broad policy, but the agencies and departments with specific authorities and responsibilities in each area will be responsible for operationally implementing that plan.

I think the overall picture, as I understand it, is centralized policy development but decentralized operational implementation because there is a number of agencies and departments that have a particular expertise or role or set of authorities that they can take advantage of.

Senator COLLINS. I share the concern of the Chairman that we do not have one person who is accountable to Congress, who is in charge of the strategy. I mean one of the problems of running it out of the White House is the individuals on the President's staff are not accountable to Congress. So for us to exercise oversight in this extremely important area becomes impossible.

I am going to push with the Chairman to continue to argue that we need one person accountable to Congress who is clearly in charge of the strategy for CVE and for homegrown terrorism. I am glad that NCTC is involved, but it sounds like everybody has a piece of it. I understand why that can be desirable, but there has to be one person in charge.

Let me, because I know we are wrapping up, switch to two other issues I want to touch on before we adjourn. I, too, am pleased to hear the priority placed on cyber security. When I look at the threats that we face that I feel we are least prepared for, cyber attacks, homegrown terrorism, and chemical/biological weapons top my list.

I read just recently a very interesting piece that General Michael Hayden wrote in which he argued that government is being too secretive about cyber security vulnerabilities, which, in turn, prevents the private sector from sufficiently addressing the threat and how to address it.

He says, "Let me be clear: This stuff is overprotected. It is far easier to learn about physical threats from U.S. Government agencies than to learn about cyber threats."

And that is one reason the Chairman and I, along with Senator Carper, have introduced a bill. It mirrors many of the recommendations of the Department of Homeland Security and the Administration to require the government to share actionable cyber information with the private sector.

I would like to ask the Secretary and you, Director Mueller, what you see as the biggest impediments to the timely sharing of cyber threat information and also cyber breaches with the private sector and with other agencies. I will start with you, Director Mueller.

Mr. MUELLER. On the one hand, there is some reluctance of the business community to share breach information with the government. That, I think, is going to be addressed, and we would want that to go to DHS and the FBI, so we can act very quickly on it.

It is interesting to see General Hayden articulating this particular view. He probably could answer the other side of it, and if he were here 2 years ago, he would have been answering the other side of it.

Senator COLLINS. That is true. I appreciated the irony also.

Mr. MUELLER. Yes, there is a very substantial imperative that to the extent possible, we share the information that will allow the private industry to protect itself from cyber intrusions to the extent that it does not disclose capabilities that we need elsewhere.

It is not only a criminal case for an intrusion in the United States, it is also often a national security risk, which we have to treat as a national security risk, and there are capabilities out there that you do not want to be disclosed because you would lose that capability.

And so, it is sometimes a difficult balancing act to make certain we push out as much information as we can, and we should. But there are some good reasons often that you cannot give as much detail as you would like, but you can give a generalized warning.

But there are some equities on the other side that we cannot go into here. I do believe—and I think the Secretary can probably address it—we are making great strides in trying to make available information that 2 or 3 years ago we would not have been able to do and are currently doing.

Senator COLLINS. Madam Secretary, do you have anything to add?

Secretary NAPOLITANO. Well, first of all, I hope the legislation moves forward. I think it is a good piece of legislation and necessary to establish authorities and jurisdiction, and the like. So we will work with you in that endeavor.

We need to keep focused on building out our information sharing capabilities at DHS through the US-CERT, through the NCIC facility and others. We have worked with the DOD on our ability to use some of the assets of the NSA under appropriate circumstances.

But the whole cyber arena, from a DHS perspective, is going to be a growth area. The information sharing with the private sector, particularly critical infrastructure aspects of the private sector, will be key for us, and then as Director Mueller said, getting information back in a timely fashion. And all of this needs to move very quickly.

Senator COLLINS. Thank you. Finally, I want to touch on the decision to make public the threat of last weekend.

The Sergeant at Arms sent out an email message to, I believe, all employees of the Senate as well as to all Senators in which he talks about the announcement and says that the announcement was "well intentioned, perhaps helpful, but not very well coordinated." This obviously worries me because the Sergeant at Arms is a key player when it comes to protecting the Washington, DC, area.

We followed up with the Sergeant at Arms. First, let me say that he said that coordination is 100 percent better than it used to be, that the FBI's local office had worked very closely with them.

But here is what he said happened. First, he was told—as we were, I might add—that the information was classified and closely held, and as he said, that is pretty typical and an understanding approach.

But then he said that the decision to go public caught them off guard. They were out of the loop, and essentially, it sounds like they learned about it on television. What is your response to this critique?

And again, so that I am not taking this out of context, he did praise the local FBI office, he did say that coordination is 100 percent better than it used to be, but he said the decision to go public took them by surprise. And that, it seems to me, should not have happened, given what a key player the Sergeant at Arms is since he controls the Capitol Police. Madam Secretary.

Secretary NAPOLITANO. It is kind of difficult to respond out of context. The decision was made to share the threat because it was credible and specific and to share it out through joint bulletins. There was a Joint Intelligence Bulletin with the FBI, to share it out through law enforcement, particularly in the affected areas, which were Washington, DC, and New York, which were the targets of the threat stream.

There was not a public elevation of the threat because the information was already getting out and actions were already being taken in response so that when he says he did not know it was going public, if he means there was some kind of public press release, there was not. There was information that was shared through law enforcement channels, as it should have been, for law enforcement to be more aware of what the threat was and what to watch for.

So whether or not he received that information, I do not know, but the information was put out through law enforcement channels.

Senator COLLINS. Director Mueller.

Mr. MUELLER. We take the position from September 11. To the extent that we have threat information and imminent threat information that is specific to a particular jurisdiction—New York, Washington, Dubuque, it does not make any difference—the per-

sons responsible for securing those communities should have the information. And we find a way to get it to them, whether it be a bulletin or through the Joint Terrorism Task Force.

Inevitably, that opens the circle of persons who have information on that threat.

Inevitably, the person responsible, whether it be in New York or Washington, DC, the police chief or otherwise, says, I have to respond to this threat. And so, you will have actions taken in each of the jurisdictions that are affected that raise the public's consciousness.

And often, as a result of the raised public consciousness, there has to be an explanation of why you are doing car stops or why you have more people on the street.

And it is that cycle where the information comes out without a conscious decision at one particular point in time—we are going to go public. The reports come in. The questions come in. And the decision is made that you have to give as much information as you can to put it in particular context.

If it has happened once, it has happened 50 times since September 11.

And if I get one criticism from State and local law enforcement officials, it is always: Director, why do I have to hear about it on CNN?

And the fact of the matter is the combination of wanting to inform people who are immediately affected by it with the understanding, as you open the circle, it is going to get on CNN probably sooner rather than later. It is a fact of life.

Senator COLLINS. It is, and I do not disagree in any way with the decision to go public because I think you want more people on the alert. I think you want the average citizen watching for suspicious activity. But it does trouble me if a person such as the Sergeant at Arms, in such a key position, did not know that there was going to be a decision made to go public.

So I would be happy to share the email that he sent to all of us with you.

Mr. MUELLER. I would like to see it, and we will be talking.

Senator COLLINS. And he does an excellent job.

Mr. MUELLER. He is terrific. He is terrific and a great partner with us.

Senator COLLINS. Let me just be clear on that, which is why I brought up his concern. Thank you very much.

Chairman LIEBERMAN. Thank you, Senator Collins.

And of course, he was previously the Chief before he became the Sergeant. So he has the background.

So it is interesting. I do not want to keep you any longer really, but there was not a decision really made, for instance in the White House, to go public with this information. There was a decision made, for all the factors you indicate, to disseminate part of the information that you had on the threat to State and local law enforcement at a for-official-use-only level, not classified. But the presumption is, based on experience, that once you do that, people are going to start talking and it is going to find its way to the media.

So have I got it right?

Mr. MUELLER. Yes, and the person, the recipient, the police chief, or others responsible for public security in that community, has to take steps.

Chairman LIEBERMAN. Yes.

Mr. MUELLER. If you take steps to respond to that threat, the question is going to be asked, why are you taking these steps?

Chairman LIEBERMAN. Right.

Mr. MUELLER. So it is a response to questions that inevitably build up as you go forward and the local communities or the Federal community take the steps necessary to address the threat.

Senator COLLINS. But, Mr. Chairman——

Chairman LIEBERMAN. Go right ahead.

Senator COLLINS. Was there not a press statement actually put out by the Department of Homeland Security? When we were briefed by John Brennan, he told us that DHS was going to be the lead on the public announcement.

Secretary NAPOLITANO. Yes, but that was later on in the sequence. That was not at the immediate time that we put out the FOUO document, as I recall.

Chairman LIEBERMAN. Good enough. Incidentally, I think Senator Collins already said this. We discussed this. We both felt that this was a case where the balance of public interest and safety was in putting this information out, not everything, but that there had been a specific, credible, unconfirmed threat.

Before we close, Senator Rockefeller has filed a statement with the Committee, which I want to include, without objection, in the record, in which he discusses the importance of allocating the D-block to first responders, and I agree with him totally.[1]

I want to thank all of you again. It is just very impressive what you and all the people who work with you have done over the last 10 years.

We are at a time of national pessimism, and a lot of it is understandable because of the economy. But it just seems to me if people in the country will think back to 9/11 and think what we have done since. We stood up two new organizations here, and the third, the FBI, was dramatically transformed. The benefit is an enormously improved homeland security.

I do not think there is another country in the world that could have done it as well as we did. Frankly, without being too explicit, there are other countries in the world, close friends of ours, who probably should have done a lot of what we did and have not yet.

But in any case, really, I think we all have reason to be grateful to you and, again, everybody who works with you on our behalf. So I thank you.

It has been a very informative and encouraging hearing. And the work is not over, as we all know, and I look forward to continuing to work with you all.

The record of the hearing will be held open for 15 days for any additional questions or statements.

With that, the hearing is adjourned.

[Whereupon, at approximately 12:38 p.m., the hearing was adjourned.]

---

[1] The prepared statement of Senator Rockefeller appears in the Appendix on page 994.

TEN YEARS AFTER 9/11: A STATUS REPORT ON INFORMATION SHARING

WEDNESDAY, OCTOBER 12, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:34 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, presiding.

Present: Senators Lieberman, Carper, and Collins.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order.

Good morning and welcome to all of our witnesses, who I thank very much for coming here today to help us review the status of information sharing among law enforcement intelligence communities at all levels of government in the United States and to determine what, if anything, we still should be doing to achieve yet better information integration and, therefore, a higher level of homeland security.

Just yesterday, we witnessed the stunning outcome of brilliant information sharing when the Department of Justice announced it had uncovered a plot to assassinate the Saudi ambassador to the United States here in the United States. The case began apparently with the Drug Enforcement Administration in Texas and Mexico before it was handed off to the FBI, and eventually to the Attorney General's Office, I presume, though it has not been explicitly said. The components of the intelligence community were also involved at various points. The system really worked brilliantly and the men and women in the field did exactly what they were supposed to do, and as a result, we are all safer, including the Saudi ambassador.

This has not always been the case, which is why we are holding this hearing. This is the ninth in a year-long series of hearings, this year being the 10th anniversary, so to speak, of 9/11, in which we are assessing progress made on key government functions that the 9/11 Commission recommended we overhaul. Information sharing was a particularly important matter to the Commission because it concluded, as we all remember, that the attacks of 9/11 might have been prevented had our intelligence and law enforcement agencies shared intelligence they had gathered and had in their possession separately to create an overall picture of what was to come on 9/11. Agencies were mired in what the Commission de-

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00269 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

scribed as a "need to know" culture for sharing information, whereas the Commission said what we should be aspiring to is a "need to share" rule.

Immediately after the 9/11 attacks, with the focus on this problem, Congress moved to strengthen information sharing among critical Federal agencies in the Patriot Act of 2001 and the Homeland Security Act of 2002. Once the 9/11 Commission released its report and its recommendations, we worked on a bipartisan basis coming out of this Committee to enact the Intelligence Reform and Terrorism Prevention Act of 2004, which tackled the problem in a comprehensive way, particularly by establishing the National Counterterrorism Center to analyze and share information to and from all agencies to better protect our homeland and by requiring the President to appoint a Program Manager in the Office of the Director of National Intelligence to coordinate information sharing across the Federal Government.

In my opinion, there is little question that our government now operates on a need to share basis much more than it did 10 years ago. As barriers of information have been taken down over the last decade, the quality, and, in fact, the quantity of information have improved and grown significantly. I think we have also integrated important new partners into the information sharing stream, and in that I mean particularly State and local agencies and the private sector, as well.

The results of these efforts are visible in game changing military and counterterrorism successes that have really protected our security. Shared information, for instance, between the intelligence community and the military led to the strikes that killed Osama bin Laden and Anwar al-Awlaki. Information sharing among Federal, State, and local agencies has played a critical role in recent arrests of homegrown terrorists, some of these really quite remarkable cases of information sharing and creativity, innovation, just plain hard work, including particularly Najibullah Zazi, the al-Qaeda trained operative who was plotting to bomb the New York City subway in 2009, and then the arrest in Seattle in June of this year of two homegrown Islamist extremists who were planning to attack a military recruiting station there.

Unfortunately, we have seen missteps, as well. Even when government officials and agencies have shared information, failure to share enough information, combined with human error and technological limitations, for instance, prevented the detection of Umar Farouk Abdulmutallab before he boarded a plane Christmas Day 2009 and tried to detonate explosives.

This Committee's January report of the murders at Fort Hood exposed more serious and ultimately deadly failure of the Departments of Defense and the FBI to share information about the growing radicalization of the alleged killer, Major Nidal Hasan, despite what our Committee investigation found were multiple red flags about his behavior.

There are other new factors that further complicate efforts to share information. For instance, the WikiLeaks disclosures exposed the risks of what might be called over-sharing without necessary safeguards. New communications technologies have made it more difficult to ensure that critical information is retained for appro-

priate use by law enforcement. And, of course, we have to ensure that information is shared in a way that adequately protects the privacy and civil liberties of our citizens.

Last week, President Obama issued an Executive Order that acknowledged that effective information sharing is critical to both national and homeland security, of course, but that in the aftermath of WikiLeaks, information must be shared in a secure manner. I think the Executive Order strikes a sensible balance between protecting information from unauthorized disclosure and coordinating information sharing across all levels of government. Now, we need to make sure the Executive Order is implemented fully and expeditiously.

So, bottom line as we meet today on this subject, I think we have come a long way since the failures of information sharing that helped to enable the attacks of 9/11, but obviously we have to continue to build on that progress if we are to maintain our security. That is what we hope this hearing this morning will help us do and why we are so grateful to have a truly excellent panel of witnesses before us. Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. I, too, am very impressed with the caliber of the panel before us, so as you were delivering your opening statement, I was trying to cut mine down so that we could get to them, since you said many of the same points.

Certainly, the results of information sharing and collaboration within the intelligence community and the law enforcement community have been evident in the operations that located, tracked, and killed Osama bin Laden and Anwar al-Awlaki in the recent months, and just yesterday in the disruption of a plot by elements of Iran's government which plotted to kill the Saudi ambassador to the United States right here in Washington. This appears to be yet another victory for cooperation across departmental boundaries.

When the Chairman and I were working on the Intelligence Reform Act of 2004, we understood that it would be challenging to change the culture in the intelligence and law enforcement communities from "need to know" to "need to share." It is gratifying, therefore, that many intelligence and law enforcement professionals have embraced this change. In a recent op-ed, the Director of National Intelligence, Jim Clapper, observed that the intelligence community now starts "from the imperative of responsibility to share in order to collaborate with and better support its intelligence consumers from the White House to the foxhole."

U.S. Attorney Patrick Fitzgerald put it more colorfully when he told an audience last month that intelligence and law enforcement operators now ask themselves, if it is found out that I have information that I did not share with someone, how am I going to justify to myself that I sat on it? He could have added, how will that failure to share be justified to congressional overseers, or far worse, to the victims of a successful attack.

I believe that the influx of new analysts that have joined the intelligence community after 9/11 has had a very beneficial impact on information sharing because this new generation of intelligence officers is much more comfortable sharing information. It is their life.

Social media and collaborative information technology have been a daily part of their lives and it is much more natural for them to share in the workplace, as well.

Notwithstanding, the many recent successes and the thwarted plots for which the intelligence and law enforcement communities deserve great credit, the GAO continues to rank terrorism-related information sharing as a high-risk area. As this Committee saw in the Fort Hood attacks and the attempted airplane bombing on Christmas Day 2009, when information is not shared, our Nation's security is placed at risk.

The Bowling Green, Kentucky, case is another recent example of information apparently not being shared and remains very troubling to me. It is unsettling that a suspected bomb maker whose fingerprints we had for many years was able to enter our country on humanitarian grounds. I have raised this issue repeatedly with the Department of Homeland Security as well as with the FBI. Both have told this Committee that the 58,000 individuals who have been resettled in the United States have been vetted now against existing databases, but what we found is the problem is that information has not been uploaded into those databases because of resource constraints. So if you are vetting people against databases that do not have all the information, you are obviously going to miss people who may want to do us harm.

But in some respects, that case demonstrates an evolution of information sharing. Originally, this information—these fingerprints that were collected from IEDs—was collected with the warfighter in mind, not with the idea of sharing them with Immigration or State Department officials to vet those who were seeking asylum. That teaches us that it is increasingly important for agencies to think creatively about other potential uses of information that we collect and how best to prioritize, analyze, and act upon that information.

Our investigation of the Fort Hood shootings demonstrated that the Department of Defense and the FBI collectively had ample information that Major Hasan had radicalized to the point where he was a serious threat, but they failed to act effectively on the many red flags.

The Chairman mentioned the WikiLeaks breach. That demonstrated that we also need to improve the security of our data from internal threats. But in doing so, we have to be vigilant that we do not recreate the old stovepipes in order to guard against the internal threat. But it is baffling to me that the individual involved in the WikiLeaks case had easy access to such a wide variety of highly classified information. Just last week, the President signed a new Executive Order on responsible information sharing prompted in part by the WikiLeaks situation. This hearing will help us assess the President's new Executive Order.

As we explore the issue of information sharing, we must also ensure that our Homeland Security partners like local and State law enforcement and fusion centers are receiving and sharing information that is useful and that adds value, and it needs to be a two-way street. Last year, this Committee passed a law that was written by former Congresswoman Jane Harman to try to guard against over-classification, and I will be interested to ask our State

and local representatives whether you have seen any benefits from that new law yet.

The public should be able to share its information, too. After all, the Times Square bombing was averted by an alert sidewalk vendor, and that is one reason that Senator Lieberman and I have introduced our "See Something, Say Something" bill, which would broaden the protections from lawsuits from citizens who in good faith report suspicious activity.

Finally, I would be remiss if I did not express my concern over this Administration's inexplicable failure to fully appoint and staff the Privacy and Civil Liberties Oversight Board that we created as part of our 2004 Act. I am truly baffled by the Administration's slowness in this regard because it is an important check as we seek to expand information sharing.

From the most sophisticated intelligence collection methods to the police officer on the street to the observant sidewalk vendor, information sharing is clearly key to keeping our fellow citizens safe.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

I thank the panel not only for being here, but for the work and thought that you put into the statements that you have prepared for this morning. The full text of all your statements will be printed in the record as if read, and we will now go to your testimony before the Committee.

First is John McLaughlin, former Deputy Director of Central Intelligence, and, for an interim period, Acting Director.

He is currently a professor at the School of Advanced International Studies at Johns Hopkins. In 2010, Director McLaughlin led an internal review for the Director of National Intelligence and Admiral Dennis Blair of the intelligence community's role with respect to the Christmas Day and Fort Hood attacks. We appreciate both your past service and the fact that you are here this morning and welcome your testimony now.

TESTIMONY OF HON. JOHN E. MCLAUGHLIN,[1] DISTINGUISHED PRACTITIONER-IN-RESIDENCE, PAUL H. NITZE SCHOOL OF ADVANCED INTERNATIONAL STUDIES, JOHNS HOPKINS UNIVERSITY

Mr. MCLAUGHLIN. Thank you, Senator Lieberman and Senator Collins. Great to see you both again.

Chairman LIEBERMAN. Thank you.

Mr. MCLAUGHLIN. The requirement to share information has been around since time immemorial, but the key thing about our time is that we are long past the moment when you can rely on a single individual or a single brain to sort through the complex problems that we deal with. In fact, today's world requires an unprecedented level of cooperation among people with varied expertise, supported by information systems that make that easier, and legal systems and procedures that take all of that complexity into account.

In formulating my thoughts on this, I am relying on two things, the experience Senator Lieberman referred to when I was Deputy

[1] The prepared statement of Mr. McLaughlin appears in the Appendix on page 1065.

Director and Acting Director in the period after 9/11, and also the work I did for Admiral Blair in 2010.

So let me begin with three positive trends, and I think both of you have alluded to some of these. First, the desire and willingness to share information is dramatically greater than it was at the time of 9/11. There are still some who resist, but the momentum is clearly in the other direction.

Second, the capabilities for sharing information have grown notably within agencies. Many are world class, but they do not operate as effectively across agency lines yet. The notable exception to this might be the National Counterterrorism Center.

Third, there is an improved policy foundation for access to and sharing of data, and I am referring to Intelligence Community Directive 501, which allows officers to discover what relevant data exists, request access to it, and have such requests professionally and fairly adjudicated. Implementation of this is moving along, though not yet complete.

But there are at least three countervailing negative trends, and again, I think you hinted at these. First, the volume of data keeps going up with no end in sight. These days, it is not uncommon at all for an analyst to see his or her daily take of messages go from hundreds to thousands overnight, ensuring that those who would do us harm do not really have to work that hard to hide. They are sometimes just lost in the noise.

Second, the breakdown in security discipline in our own government works against sharing of information, and you both alluded to this. Leaks, authorized and unauthorized, reinforce arguments made by those who stress the risks of sharing and pose obstacles to doing so.

And third, despite the progress represented by Intelligence Community Directive 501, broader policy procedure and law have been a little slow to keep pace with the challenge.

So given that complicated picture, what is the way forward? Above all, we need finally to break through the barriers that have for years kept us from bringing the most advanced information technology to bear on the problem. Information technology can prompt humans to look in the right places, consider pieces of data that might otherwise be missed, expose relationships that are buried in all the noise that the avalanche of data represents. What stands in the way? There are three major issues.

First, there is in the national security community limited visibility into data that is distributed across multiple agency systems housed in different agencies.

Second, existing search capabilities do not allow for exploitation of existing data.

And third, I am not sure there is a common and widely shared vision among national security specialists on the end state they want to achieve here.

There are a number of things that deserve attention in the near and medium term. In the near term, it is important to strengthen online instruction for national security specialists on what data exists. Sometimes, they do not know.

In the medium term, we should work to improve search capabilities and training in how to use them.

And in the longer term, and once basic capabilities are improved, we need more software capable of exposing the underlying relationships in large bodies of data.

Faced with challenges like this, one key need is a common standard across the intelligence community for access to data, essentially, the virtual equivalent of a community badge that now allows officers to move physically from agency to agency. This would mean, for example, that when someone logs on in one agency, other agencies whose data that person is seeking would confidently know who this person is and what they are authorized to access. It is easier to say than do, but it is achievable over time.

Another broad problem likely to complicate our efforts, especially the need to identify people involved in terrorism, is that so many of them are turning out to be Americans. Names like al-Awlaki, Najibullah Zazi, David Headley, Faisal Shazad, and just yesterday, Manssor Arbabsiar, are familiar ones in this room. This is a problem with at least three dimensions.

First, I suspect there is still an inconsistent understanding of the laws and regulations that govern the acquisition and sharing of data that touches Americans—these are complicated laws.

Second, there is an understandable concern not to violate the laws protecting our citizens' privacy, and this can inspire a subtle kind of risk aversion in dealing with such data. We saw this in some cases I have looked at.

Third, terrorists, in my personal view, have figured all this out. Faisal Shazad, the unsuccessful Times Square bomber, got his citizenship here within the year before he attempted to carry out that act. This tells me that these people know that complicates our task in detecting them.

Finally, I would just say that any misgivings we have about counterterrorism stand out, and I think you both alluded to this because they are so at odds with the broad pattern of success we have experienced since 9/11. Our law enforcement, intelligence, and military officers have really delivered. As always, intelligence successes are rarely apparent, not only because we cannot talk about them, but because they are often woven kind of invisibly into the fabric of successful policy.

Those are my opening thoughts on this. I thank you for the opportunity. There is a fuller statement in the record, but these are the basic points I wanted to make. Thanks.

Chairman LIEBERMAN. Thank you very much. Those were excellent opening thoughts.

Ambassador Ted McNamara served as Program Manager for the Information Sharing Environment from 2006 to 2009, where he had lead responsibility for coordinating the Federal Government efforts with respect to information sharing. It is a pleasure to welcome you back to the Committee and we look forward to your testimony now.

TESTIMONY OF HON. THOMAS E. MCNAMARA,[1] ADJUNCT PROFESSOR, ELLIOTT SCHOOL OF INTERNATIONAL AFFAIRS, GEORGE WASHINGTON UNIVERSITY

Mr. MCNAMARA. Thank you, Mr. Chairman. Thank you very much. Let me start by saying that during my 3½ years as a Program Manager for the Information Sharing Environment, I had the pleasure to work very closely with Members of this Committee and the staff and I received nothing but encouragement, constructive criticism, and strong bipartisan support, and for that, I want to thank the Committee, especially the Chairman and Senator Collins. The two of you are unsung heroes of what we got done downtown.

I think what you probably would like to see from me is the view from the trenches. I will try and do that.

Two years ago, in my final appearance before the Committee as the Program Manager, I stated that we had built a strong foundation for the ISE, but that a fully functional and mature ISE was still in the future. I am delighted to observe that 2 years later, we have gone well beyond that point.

A truly mature and functioning ISE can only exist when we have fully standardized and harmonized rules, procedures, and operating systems to manage the ISE. To get from the start point to that fully mature system, we now know, as we were not fully aware of back in 2005, is a long, complex, and difficult process. Today, 10 years after 9/11 and 5 years after I sent the required Program Manager's first implementation plan to the Congress, we are well beyond the foundation, but we are not near the finish.

What I find most encouraging in the last 2 years is that the pace and breadth of the change are stronger, more widespread, and exist among all stakeholders. Concepts and programs that were hard-fought struggles in those first years are conventional wisdom now. I will give as one example, the Controlled Unclassified Information program. It was met with widespread skepticism and open opposition in 2006 when we set the goals for building it. Today, there is not a single agency I know of that opposes the CUI or believes that the old way was better. From my perspective, that is a huge progress.

At the macro level, my observation is that the ISE is alive, well, and growing stronger. We spent a lot of time getting buy-in from the stakeholders. I would equate what happened with the proverbial supertanker that takes so much time initially to start turning, but once it turns, the turning is quite forceful. The problem for the manager, or in this analogy the captain, is to make sure the turn winds up on course. I think that we are on course. We still have, however, incomplete standardization and harmonization. They are central problems, still, today.

We also have another problem which I did not face, and that is as the ISE grows, it begins to bump into other programs and priorities which are out of step with it and which have major conflicting priorities. A growing ISE interferes with other big rice bowls. I would say that the incomplete standardization and harmonization,

[1] The prepared statement of Mr. McNamara appears in the Appendix on page 1073.

and the bumping into other priorities are two of the major causes of the WikiLeaks problem. There are a couple of others.

What happens, and what happened in the past, I believe, has been a transformation of attitudes. We have all seen the absolute necessity now of managing information in the new information age in a way that responds to the need of that new age. Let me list just a couple of things that I think were important to what we have done: A national network of fusion centers, the Controlled Unclassified Information that I have already mentioned, Suspicious Activity Reporting, National Information Exchange Model, and what I am particularly proud of, the privacy and civil liberties protections. All of those are accomplished, they are functioning programs.

Let me list a few things that I believe are high priorities, which still remain. Although all of them have started down a path, they have a much longer way to go. First of all is monitoring and auditing. We are not monitoring and auditing the system with the technology that is available and in the manner in which we need to do it, which is another reason for the WikiLeaks.

Second is discovery and authorized use. It is beginning in the various communities, those stakeholders that I mentioned earlier, but it is not yet a unified and standardized system.

Interoperability across networks—again, it has begun, but there is a long way to go. The technology is there; we just have to spend the time and the resources to get it implemented.

And finally, we need to expand the mandate, something I said in my last address to this Committee and to other congressional committees. It is time to expand the mandate of the Program Manager. It is not possible to set up an Information Sharing Environment only for terrorism information. It will not work.

I will close by summing up what I think can be the future of the ISE. We have built the foundation. Two years ago I borrowed the Churchillian phrase that we were not at the beginning of the end, but we were at the end of the beginning. I think we have gone beyond that now. I would estimate that we are about halfway there. Quite a bit of progress.

It took us 5 years to get to this point. Fortunately, because of the changed attitudes, because of the increased pace and breadth of the changes that are going on, I do not think we need another 5 years to get to our goal of a fully functioning and fully mature ISE.

And with that, I will close my remarks. Thank you.

Chairman LIEBERMAN. Thanks very much, Ambassador. That is very encouraging. Thanks for the part that you played in the progress that we have made in this area.

Chief Cathy Lanier is, of course, the Chief of Police of the D.C. Metropolitan Police Department. As such, she has been a leading advocate for the importance of effective information sharing with State and local law enforcement and has had direct experience on the effectiveness of information sharing regarding various terrorist threats in Washington, DC.

Chief, thanks for taking the time to be here. Good morning.

TESTIMONY OF CATHY L. LANIER,[1] CHIEF OF POLICE, METROPOLITAN POLICE DEPARTMENT, DISTRICT OF COLUMBIA

Chief LANIER. Thank you for having me here. Good morning, Chairman Lieberman, Senator Collins, Members of the Committee, staff, and guests. Thank you for the opportunity to present this statement on the status of information sharing among Federal and local partners.

Of course, I am the Chief of Police here in Washington, DC, of the Metropolitan Police Department. I would like to remind everybody, that is the primary law enforcement agency here in Washington, DC. As the chief of police of a major city police department, I am very pleased to be able to brief you on the significant progress that has been made in the Federal and local information sharing and how that has improved our ability to safeguard the public.

In my testimony, I will elaborate on why it is even more important now, 10 years later, to recognize the vital role of law enforcement in our homeland security efforts. With threats to the Nation constantly evolving, local law enforcement officers who are on the street every day are uniquely positioned to detect and prevent terrorist incidents.

There are more than 700,000 law enforcement members across the Nation that know and are well connected to the communities that they serve, placing them in the best position to detect and investigate criminal activity that might be connected to terrorism or violent extremism. Clearly, information sharing with local police is essential to countering the threats that we face going forward.

The success of local law enforcement in fulfilling our role hinges on the cooperation and support of our Federal partners. Ten years after the September 11 attack on the United States, the partnership between Federal and local authorities is very robust and continues to improve. The 10-year anniversary of 9/11 presented an excellent case study to illustrate how the infrastructure and relationships that we have built operates in a critical situation.

Important groundwork for the anniversary preparations was established in 2010. With a significant increase in American residents aligned with violent Islamist extremists who are arrested or convicted in 2009, the Department of Homeland Security launched a broad working group on countering violent extremism. From the outset, the working group included local law enforcement. Following that effort, the Department of Homeland Security and the FBI committed to a partnership with the Metropolitan Police Department to go out and engage and educate our partners in the private sector and the community. Beginning in 2010, we jointly briefed literally thousands of government and private sector partners around the National Capital Region on recognizing and reporting suspicious activity as well as responding to potential terrorist incidents. Those briefings certainly paid off, as you will see, when we entered the high-threat period of the 9/11 10-year anniversary.

Let us fast forward to last month. Early on the morning of September 8, 2011, I received virtually simultaneously calls from both my own official on the Joint Terrorism Task Force and my counterpart at the Department of Homeland Security urging me to attend

[1] The prepared statement of Chief Lanier appears in the Appendix on page 1078.

a classified briefing on an emerging threat to Washington, DC, and New York. Within an hour, both the FBI and DHS provided me with unfettered access to the actual cable outlining the threat. I continued to receive up-to-the-minute briefings from the FBI over the next several days. This was critical, as I continually had to make staffing and deployment decisions on a shift by shift basis. This shows that not only have we built strong relationships in the region, but more importantly, the institutional structures that we have created are ensuring the flow of information.

What perhaps was even more important was the quality of the information that was made available to me. The details in the briefings were far greater than we had received in the past and enabled me to focus our officers very specifically on threats.

Equally important, within 24 hours, the intelligence community collectively decided that the public needed to be informed of this credible threat, a significant departure from previous experience. This decision helped law enforcement in several ways. For one, many of the actions of local law enforcement, as you know, are much more visible than that of our Federal partners, and in many cases, they are intended to be. In other words, our community members notice when we take steps in relation to heightened threats. They see us on the street, they see us around critical infrastructure, and they know something unusual is happening. Although this may only be a local concern, announcing the threat helps local authorities explain, and sometimes justify, our actions to the public. Local partners really appreciate that support.

More importantly, making this potential threat public helped us focus our community on reporting the types of suspicious activity that may help us detect and deter those who may be interested in carrying out this threat. Obviously, when we can effectively harness and direct the attentions of the public, we can get much more useful information to help us counter that threat.

In this case, just after the announcement to the public, our calls for suspicious activities jumped significantly. Most importantly, this announcement calls many of our private sector partners that we had educated in the joint briefings much earlier to start reporting suspicious activity that warranted further investigation.

For example, on September 10, the Metropolitan Police Department was contacted by the general manager of a local hotel who advised that six males from various Middle Eastern countries had checked into the hotel between September 8 and 10. The last to arrive paid cash for the room, asked for a specific view of a notable landmark. All six placed "Do Not Disturb" signs or placards on their doors.

A manager at another hotel contacted the MPD on September 11 to report that cleaning personnel had found suspicious items left in a hotel room. The occupant had departed early without checking out and leaving cash for the room. In this instance, the activity was linked to suspicious financial transactions that had been reported to the MPD earlier in the week. The MPD and the FBI determined that the case did not have an actual nexus to terrorism. However, it was linked to criminal activity.

Although neither instance was related to the 9/11 threat or to terrorism at all, the hotel managers in both cases took the right

steps in calling the police to report these indicators. As you can see, providing some of the information to the public helps our efforts in the long run. It is a recognized principle in policing that sometimes you need to give a little information to get information.

With the information about the threat on the anniversary of 9/11 and the visible government mobilization to it, the public is reminded of the importance of sharing information about suspicious activities. It also reinforces the significance of our "See Something, Say Something" campaign, which has been strongly supported by Federal and local partners.

Fortunately, our experience here in the District of Columbia during the threats of 9/11 highlighted several areas where information sharing has improved. However, in recognizing that my experience here in Washington, DC, does not represent all police chiefs, I did reach out to the major city chiefs and former Chief of the MPD, Commissioner Charles Ramsey, who is now the current Commissioner in Philadelphia, to see what other chiefs around the country are seeing. What we are seeing across the major cities is that there has been significant progress since 9/11. One person simply and aptly described the fusion centers and the FBI's field intelligence group as game changers for local police departments. We would not be able to prepare for and work together to prevent significant threats facing our communities without this sea change in government cooperation. In addition, these cornerstones of Federal-local information sharing, we continue to work on new links between levels of government and the private sector.

In the interest of time, I will stop there and you have my full statement on record.

Chairman LIEBERMAN. Thanks, Chief. That was great. Just a quick question. Is your main point of contact with the Federal Government, the Department of Homeland Security?

Chief LANIER. Typically, most of my information comes in through the FBI.

Chairman LIEBERMAN. OK.

Chief LANIER. We have heavy participation on the JTTF and I have daily conversations and twice-a-week briefings from the JTTF.

Chairman LIEBERMAN. Good. Thank you.

Our next witness is Ron Brooks, another important part of this newly established framework for information sharing and homeland security, the Director of the Northern California Regional Intelligence Center, which is the fusion center for the San Francisco Bay area. Mr. Brooks is also the Chairman of the Criminal Intelligence Coordinating Council, which is a State and local advisory group to the Federal Government on information sharing issues, so he is uniquely qualified to testify today.

Thank you for coming across the country to be with us.

TESTIMONY OF RONALD E. BROOKS,[1] DIRECTOR, NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER

Mr. BROOKS. Thanks, Mr. Chairman and Senator Collins. I appreciate your continued attention to this important issue and for

[1] The prepared statement of Mr. Brooks appears in the Appendix on page 1085.

inviting the National Fusion Center Association to provide our views.

Mr. Chairman, we are light years ahead of where we were on 9/11. In fact, we have moved really beyond information sharing to create a true homeland security enterprise. Providing for the common defense is a Federal constitutional responsibility, and in post-9/11 America, the national network of fusion centers plays a pivotal role in helping the Federal Government achieve that important goal.

Fusion centers are much more than information sharing hubs. They embody a process, the fusion process, that has fundamentally changed how information is gathered, transformed into actionable intelligence, and shared over both classified and unclassified networks. They are about putting national threat information in a local context for action by leveraging the 840,000 law enforcement officers on the ground to support the national security mission. Without fusion centers, there is no mechanism that allows us to do this across all 50 States.

Last month, less than 24 hours after high-level national intelligence indicated a 9/11-inspired threat, detailed information was sent through DHS and FBI to the fusion centers and was put in the hands of local law enforcement. Fusion center analysts across the Nation worked around the clock alongside FBI and DHS personnel to review suspicious activity reports and leads associated with the New York and Washington, DC, threats and to share actionable intelligence with decision makers at all levels.

This is much more than information sharing. It is deep collaboration, and it is essential to effective homeland security and it is impossible to do without the National Network of Fusion Centers. In addition to information sharing, fusion centers give us complex analytic capabilities. Fusion centers have the ability to catalog critical infrastructure, leverage a large network of trained terrorism liaison officers to report suspicious activity, overlay that SAR data on critical infrastructure and layer in national threat information. The result is high quality actionable intelligence.

None of this was possible on 9/11. Even at the Federal level, agencies do not have the manpower, local knowledge, or trusted partnerships to handle such an effort, yet it is happening every day at fusion centers and that adds tremendous value to the Federal Homeland Security Enterprise.

Last October, an advisory was distributed by the New York Police Department concerning a suspicious truck whose driver reportedly diverted its route toward Times Square in exchange for $10,000. After DHS informed several fusion centers in the region, analysts at the Rhode Island Fusion Center discovered that the owner of the truck was a California native and coordinated with my fusion center to conduct background checks. Within 2 hours of the initial advisory, information from those two fusion centers was used to coordinate with the Connecticut Fusion Center, which enabled the State Police to locate and stop the truck before it reached New York. If not for the National Network of Fusion Centers, the dedicated personnel from DHS and the FBI, we could not have moved from alarming SAR to a threat resolution within just hours.

Not only do fusion centers enable the Federal counterterrorism mission, the all crimes approach generates value in communities every day. This past July, an alert from the Oklahoma Fusion Center referenced a suspect wanted in connection with a double homicide who was trying to escape to Canada. The North Dakota Fusion Center analyzed the suspect's vehicle and information and connected with the Arkansas Fusion Center, which quickly provided a photo of the suspect. The fusion center released the information in an alert to law enforcement, who apprehended the suspect that same day. Again, fusion centers were essential to a quick resolution.

The National SAR Initiative is being implemented across the National Network to gather and analyze tips and leads for analysis of suspicious activity that might be linked to terrorism. Fusion centers are linchpins in the implementation of the Nationwide Suspicious Activity Reporting Initiative. Without fusion centers, we would not have a portal for the SAR process or a system that provides SAR-related front-line officer and analyst training. We would not have a way to share or request information among the JTTFs, DHS, and local public safety partners. We would not have the ability to vet SARs through a national standard that protects civil rights and civil liberties according to the ISE-compliant privacy policies that are now enforced in every fusion center.

The value of fusion centers is clear, but that value is at serious risk. Urban Areas Security and State Homeland Security Grant programs, the primary DHS programs that support fusion centers, have been slashed. Each fusion center is operated by State and local governments. Some centers rely heavily on Federal funding while others rely on funding from their own States. In all cases, State and local agencies make major contributions of full-time personnel that are not reflected in that budget data.

After 9/11, much of the Federal assistance to State and local partners supported enhancements to response capabilities. It is time to reinvest in enhancements to prevention capabilities in a more focused way, and that includes supporting fusion centers. Unless Congress and DHS take measures to focus State and local assistance on fostering prevention capabilities, the forward progress that we have made on information sharing and SAR reporting could be reversed.

Mr. Chairman, we have learned some tough lessons. It is easy to focus on mistakes when they are made, and unfortunately, we probably will not stop 100 percent of the threats to this Nation. But the grassroots development of this decentralized national network of fusion centers, really, that distributed and decentralized system that was called for in the Intelligence Reform and Terrorism Prevention Act, is a tremendous accomplishment. It is generating value every day and has become a true national homeland security asset.

On behalf of the National Fusion Center Association, we commend your leadership and the leadership of this Committee and ask for your continued support, and I have submitted my full remarks to the Committee.

Chairman LIEBERMAN. Thanks, Captain Brooks. I am a strong supporter of the fusion centers. I appreciate the case you made for

them, as it were, and I have one or two questions in that regard when we get to that point.

Finally, Jeff Smith is a partner at the law firm of Arnold and Porter, former CIA General Counsel, a familiar and trusted source of counsel for this Committee and me personally. Mr. Smith is testifying on behalf today of the Markle Task Force for National Security, which released a series of reports over the last decade that played a really seminal role in shaping the policy debate on information sharing.

So, counselor, we welcome you back.

TESTIMONY OF JEFFREY H. SMITH,[1] PARTNER, ARNOLD AND PORTER

Mr. SMITH. Thank you, Mr. Chairman, Senator Collins, and Senator Carper, for holding this hearing and for your leadership on this critical issue. I appear this morning on behalf of the Markle Task Force on National Security in the Information Age. My prepared statement is jointly submitted with Zoë Baird Budinger, the President of the Markle Foundation.

I want to begin, as my colleagues have, by commending this Committee and your staff for the significant time and energy you have devoted to making information sharing a top national priority. The work of your Committee has helped make this Nation safer.

Since 2002, the Markle Task Force has worked hard to provide policy makers, including this Committee, with recommendations to help accelerate our government's use of information technology to better understand the threats we face, to make better decisions, and at the same time protect our national and vital civil liberties. I am pleased to say that many of our recommendations have been accepted.

As a result of all of these efforts, substantial change has occurred throughout government. Information sharing has become more widespread. That said, progress has been too slow in some places and has lacked adequate guidance or oversight in others. Information sharing is like the blocking and tackling in football. It is not as sexy as a 60-yard pass to a wide receiver, but at the end of the day, it wins games.

Ten years ago, there was a failure to adapt to a network world. Our law enforcement and intelligence communities were driven by the "need to know" culture that stovepiped information. This was in part because of the so-called wall between law enforcement and intelligence. This failure to connect the dots has become famous since 9/11, but that phrase oversimplified a fundamental problem, not only with the sharing of information, but with the way in which departments and agencies worked together.

Where are we today? Washington can work, as demonstrated by the changes that we have talked about and this panel has talked about. We have had three dramatic successes: The attack that led to the death of Osama bin Laden; Najibullah Zazi was arrested on September 29, 2009, in connection with an al-Qaeda plot to bomb the New York City subway system; and on May 1, 2010, because of improved watchlisting procedures, Faisal Shazad was success-

[1] The prepared statement of Mr. Smith appears in the Appendix on page 1107.

fully apprehended after his attempt to detonate a car bomb in Times Square. He was arrested 53 hours and 20 minutes after he left Broadway, largely as a result of better sharing and cooperation with State and locals.

But we still fall short. The task is enormous. Where should we be going?

The Markle Foundation Task Force has four critical steps that we recommend. One is strong leadership from the highest levels of government is required to sustain the progress since 9/11. There is a risk that this virtual reorganization of the government will be eroded as a result of bureaucratic turf battles and fears about information security.

Two, the adoption of discoverability and authorized use must be expanded. It is possible for relevant data to be discovered in an automated manner that allows both human users and data itself to find relevant information. This is often referred to as data finding data. The concept of authorized use is being adopted, but it must be expanded. An important Intelligence Community Directive, ICD 501, was issued in 2009 that represents a substantial step toward enhanced discoverability and authorized use. Ambassador McNamara talked about that and the importance of that needs to continue to be pressed.

Three, privacy and security protections must be increased simultaneously. WikiLeaks is not an argument for less information sharing. Doing that would compromise our national security. As we improve our capabilities to better share information, we should simultaneously deploy better policies and technologies to control its access and use. I am pleased with the new Executive Order the President signed on Friday. It was a significant step in the right direction and I look forward to discussing it with the Committee.

I also share Senator Collins' concern about the failure to appoint persons to the Privacy and Oversight Board. It is a frustration, and I am happy to talk about that.

Developing this trust is critical so that the American people will trust that the government will protect its civil liberties. It is important so that government officials will share information with one another, confident that it can be kept confidential.

The fourth point is one that a couple of people have made, including Ambassador McNamara. Information sharing is a tool that can help make the entire government more efficient. The trusting sharing of information in government decisionmaking is not a unique attempt to counter terrorism. Successful information sharing is a model that can be used across many areas of government to improve the effective functioning of government.

Mr. Chairman, that concludes my remarks. I look forward to your questions.

Chairman LIEBERMAN. Thanks very much for that testimony and for your work with the Markle Task Force.

We will do 7-minute rounds of questions.

Ambassador McNamara, let me pick up where Mr. Smith ended. I wonder if you could just say a bit more about why you think it would be valuable to expand the authorities of the Program Manager for the Information Sharing Environment and how you would do it.

Mr. MCNAMARA. Well, let me go back to the very first year I was on the job. It was apparent that we were not going to be able to, for example, create a Controlled Unclassified Information system, which only handled terrorism information. No agency managed their data in that manner. So when we sat down to do CUI, we created CUI for all controlled unclassified information.

I only had the authority to mandate it to the agencies for terrorism. Fortunately, terrorism was a high enough priority that they had to pay attention to me. But, in fact, only a very small portion of CUI information, I would say a single-digit percentage, is terrorism information. Most CUI, and it goes all the way down to State and local authorities, is unrelated to terrorism. Yet the system works for all of it. We had to build it that way or it would have failed.

Another example is the Suspicious Activity Reporting. When I picked that up off the ground, and turned it into—I should not say "I," I should say "we," because there was an awful lot of partners that were helping us. We had to do it for terrorism information. But as I have said so many times, if you take the Suspicious Activity Reporting mechanisms and you unplug the database that says "terrorism information" and plug in one that says "serial killers," or unplug that and plug one in that says "drug violence," or unplug that, you name it, it works for all suspicious activities. In fact, we constructed that knowing that if it only worked for terrorism information, it was not going to last. It would be too small and disappear.

Another example is the fusion centers. There is only one fusion center in the United States that handles only terrorism information and that is the National Counterterrorism Center. The others all handle all crimes and all hazards.

Chairman LIEBERMAN. So how far would you expand the——

Mr. MCNAMARA. I would like to see that an Information Executive be created, probably in the Office of the President, as a manager, not a crisis manager, as I was, in the Program Manager position.

Chairman LIEBERMAN. Right.

Mr. MCNAMARA. Not doing just a program, but managing information the way a Chief Information Officer does it, across the board, with complete authorities. You have to give that individual some budget clout. I had virtually no budget clout——

Chairman LIEBERMAN. Right.

Mr. MCNAMARA [continuing]. So I had to appeal for agencies to do it. And the person needs to work very closely with OMB and with the agencies as an overseer, not a doer.

Chairman LIEBERMAN. That is helpful. Is your preference that this be done by executive action, or do you think it requires legislation?

Mr. MCNAMARA. It does not require legislation, as far as I am concerned.

Chairman LIEBERMAN. Good. I say good because——

Mr. MCNAMARA. But it may require some congressional push to get the executive action.

Chairman LIEBERMAN. Well, we are glad to do that. We generally categorize that as oversight.

Director McLaughlin, in your testimony, you note the growth in the number of Americans participating in terrorism, which has been a focus of our Committee, and that reality creates a set of challenges for the intelligence community given rules in place related to the acquisition and sharing of data that touches U.S. citizens, and I am quoting from your testimony. We have strong rules in place to protect such U.S. persons' information within the intelligence community, but you note that this can lead, and I agree, to, and I quote again from your testimony, "a subtle kind of risk aversion in dealing with such data."

So talk to us in a little more detail about that. What kind of risk aversion are you worried about, and do you think the intelligence community needs to clarify the framework that it is operating under now for dealing with information regarding U.S. persons?

Mr. MCLAUGHLIN. I do, Senator. This comes directly out of the study we did for DNI Blair in 2010.

Chairman LIEBERMAN. Yes.

Mr. MCLAUGHLIN. We talked to people in a dozen agencies and carried out about 70 interviews, and one of the things that came out of that, because in both the Christmas bombing and in the Fort Hood shootings you had the involvement of an American citizen at some level—that was Anwar al-Awlaki having inspired the Christmas bomber and having played a role in his communications with Major Hasan—what we discovered was that as you went agency to agency, you got different interpretations of what was allowed and not allowed when you encountered U.S. persons' data. And people, frankly, were very careful, particularly at the National Security Agency, where this is most likely to occur, and this results, in part, from some of the controversies involved with their collection programs and so forth that you are familiar with.

Chairman LIEBERMAN. This is the risk aversion——

Mr. MCLAUGHLIN. This is the risk aversion part of it.

Chairman LIEBERMAN. In other words, to avoid the risk, they may not be going some places we would actually want them to go in terms of——

Mr. MCLAUGHLIN. Well, the way I would put it is that we certainly were not pushing them to violate anyone's privacy.

Chairman LIEBERMAN. Understood.

Mr. MCLAUGHLIN. What we came away believing, and I had a civil liberties attorney on my task force, was that in many cases, intelligence agencies were not going to the limit of what the law allowed them. In other words, they wanted to err on the side of not ever crossing that line. And some, frankly, confessed worrying about punishment of some sort if they did cross that line.

Chairman LIEBERMAN. Sure.

Mr. MCLAUGHLIN. And without going into the classified details of that study, I think we came to the conclusion that this was one of two big reasons why we did not anticipate or detect Abdulmutallab's intentions here—because as a former intelligence officer, I know how these things can get kind of oversimplified, but I came away reluctantly convinced that had we been more aggressive on this particular score and had we also had information technology that helped the human brain connect things up——

Chairman LIEBERMAN. Right.

Mr. MCLAUGHLIN [continuing]. We would have found this guy and we would have known pretty much what he was intending to do.

Chairman LIEBERMAN. Well, that is a very important conclusion.

Mr. MCLAUGHLIN. Another part of this, if I could just add this final point——

Chairman LIEBERMAN. Go ahead.

Mr. MCLAUGHLIN [continuing]. Is that sometimes, and this, I have to be a little careful with because there is some sensitive stuff involved, but sometimes foreign partners encounter information about American citizens and they are often confused about what do we do with that because it is sensitive. So that is another area that needs to be clarified.

Chairman LIEBERMAN. Do you know whether any changes have been made as a result of your report?

Mr. MCLAUGHLIN. I know the recommendations were taken seriously and I have been told by people at the White House that they are working on this. I checked within the last 24 hours and I think people are sensitive to the question, but I would say that it probably is something that still needs to be worked on, primarily by someone like the DNI and the Department of Justice convening people throughout the intelligence community who have the job of interpreting these regulations to the workforce and making sure, as a first step, that they are all on the same page, that everyone is getting the same message.

Chairman LIEBERMAN. That is very helpful and I promise you that we will take this on in the Committee as another kind of oversight responsibility because of the rising significance of terrorism committed by American citizens or legal residents of one kind or another. My time is up. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I am going to continue with Director McLaughlin exactly along the lines of what you just started because we have now talked a little bit about the Abdulmutallab case, and by the way, I am informed that he pled guilty today. But our Committee also looked at the Major Hasan case and the information sharing or lack thereof in that case, and it was fascinating to talk to the members of the Joint Terrorism Task Forces both in Washington and in San Diego and to learn that they chose not to share all the information that they had due to the requirements for FBI approval for sharing under the JTTF guidelines and the Memorandum of Understanding. And thus, you had a situation, without going into classified information, but let me say it was widely reported, of contacts with al-Awlaki that were not passed on to the Army, because even though there was a member of the Department of Defense represented on the JTTF, because it could not be passed on without explicit approval by the FBI.

Did your committee, in looking at these cases, take a look at whether those guidelines and Memoranda of Understanding that applied to the JTTF's information sharing with the home agencies need revision, as well?

Mr. MCLAUGHLIN. We did. We were a little limited in what we could do on the Fort Hood case because there were some ongoing legal questions that inhibited our ability to interview everyone who

was involved, but we did speak with enough members of both San Diego and Washington to come to similar conclusions, and the main conclusion we came to was that no single person had looked at all of the information. Some of it had been seen in San Diego. Some of it had been seen in Washington. And there were some follow-up issues that you are probably familiar with that were not as aggressively pursued as should have been.

The main thing I was concerned about was if someone has done something about this, and I got assurances from both the FBI and the Department of Defense that they now have a way when something like this occurs to pass information that was not—the kind of information that was not passed in the Major Hasan case—to counterparts in law enforcement, or vice-versa, from law enforcement to counterparts in the Defense Department.

I think I came away as pretty much assured that they have figured that out. Now, that is always fighting the last war, so you always have to ask, are there other realms, other circumstances in which that same issue might arise, and I think we need to keep our eye on that across the board.

Senator COLLINS. Thank you.

Ambassador, we have just talked about policy obstacles in the form of restrictions through guidelines or Memoranda of Understanding that may restrict information sharing. From your perspective, how much of this is a policy problem versus a technical problem? I remember the first hearing that we held after the Abdulmutallab case, and the deputy from the National Counterterrorism Center told us, much to my amazement, that they lacked the technology to do the kind of federated searches that were needed, which amazed me because all of us who go on Google know that if you type in a name and it is not quite right, you get the question, "Did you mean X?" and any of us who have ordered on Amazon have seen how information of, you might like this, that is similar. So it seems like the technology is out there to be used.

What is your assessment? Is this a technology problem? Is it a policy problem? Is it still a cultural problem? A leadership problem?

Mr. MCNAMARA. That is an excellent question. First of all, it is not a technology problem, strictly speaking, if you mean by technology the availability of the technology. That is there.

The policy problem is that the policy does not allow the technology to work or to be employed because of policy restrictions. Then, the attitudinal problem ("in the trenches" problem) comes when, even though you change the policy, the work habits and the ingrained methodologies of those working do not change.

So, I have not seen, in all of the years I have been involved in this, a true technological problem. In addition to these problems you have the resource problem. So if NCTC says that it does not have the technology to do the integration of the data, it is not because integration technology does not exist, which can be either taken off the shelf or modified and used. It is because policies do not allow them to use that technology, or resources are such that they cannot afford to put it in until later.

To move out from the Federal Government, I found, and I cede to both Ms. Lanier and Mr. Brooks as to whether or not my vision

of this is still accurate, but I believe it is. There are ingrained habits that persist. I am not going to pick on the FBI or DEA or law enforcement, but if you think about the need to integrate the activities of the fusion centers with other fusion center-like activities out there, such as JTTFs and HIDTAs, there is no reason why those organizations should not be collocated. As Mr. Brooks referred to, he was having what he called "deep collaboration." But that only comes with collocation and with some form of integration of activities.

I looked at the statistics. There is fewer than one full-time FBI agent, on average, at fusion centers around the United States. That is liaison. That is not full collaboration. Now, I know in the large cities—possibly here in Washington, DC, New York, and other places—that is not the case. It is a much closer collaboration. But the habits, the ingrained habits, when not changed by the policy, the resources, or not changed by the leadership, results in situations where the information does not get shared. I know of no tech problem that stands in the way.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thank you, Senator Collins. We will do one more round of questions.

Chief, I was interested when you said that your main point of contact with the Federal Government is the FBI. From our perspective, there is nothing wrong with that, of course. I will say that when we created the Department of Homeland Security, and particularly creating within it the Intelligence and Analysis Section and watching it evolve, one of our hopes, and I think Secretary Napolitano's hopes now, for I&A was that it would play a very important role, unique role in the intelligence community in both transferring and receiving intelligence from State and local law enforcement.

In fact, DHS and FBI have been working very well together, but I want to ask you this. One of our visions here, and it was not just ours alone, was that we have hundreds of thousands of State and local law enforcers, etc., across the country, that they, if properly informed, alerted, or involved, would become hundreds of thousands of additional eyes and ears in our effort to protect the homeland, particularly from terrorist attack. And, of course, if that was true anywhere because of the centrality of Washington, DC, it would be here.

So my question is whether you think, as the Chief of Police here in Washington, DC, enough has been done to encourage information sharing from your force, up as opposed to from the Federal Government down?

Chief LANIER. Yes.

Chairman LIEBERMAN. I think you have testified in very encouraging ways to the way in which there has been cooperation and more sharing from the Federal Government down, but how about from the local level up?

Chief LANIER. That is actually a very good point, and particularly with the threat that we see evolving now of so many American citizens and people living in the United States becoming part of this threat because people call the police and report all kinds of strange

behavior by neighbors or people in the communities and they call us with that.

Chairman LIEBERMAN. Right.

Chief LANIER. So the way that works, and I want to back up and clarify a little bit—I have a large contingency of officers assigned to the JTTF and I receive twice-a-week briefings from them, and they have full access to cases they are working here in the NCR—which are most important to me—or anything relevant to Washington, DC. So that is why I say that, primarily, the information I get on the counterterrorism side comes from the FBI.

However, when there are threats or different things that are going on, DHS does a very good job, and I&A, in putting out those intelligence bulletins. They have an analyst in my fusion center who works with all of our other analysts that continually produce products for us and for us to share with our forces to do what you described, updating our local police officers to know what to report.

In terms of two-way information, we started the SAR Initiative that was talked about by Mr. McNamara 3 years ago and has now evolved so that we have a way to receive suspicious activity reporting through text messages, 911 calls, email, and we just launched iWatch, which is a community public reporting tool, so people can report suspicious activity. We also have engaged with Trap Wire, so when those SARs or those suspicious activities come in, they come into the fusion center, enter into the system that we have, Trap Wire. They are first reviewed by analysts in the fusion center. Then there is an analytical software that also analyzes those suspicious activity reportings and there is a decision made there whether it should be bumped up into eGuardian, which is shared space——

Chairman LIEBERMAN. Right.

Chief LANIER [continuing]. So we can connect the dots with suspicious activity reporting around sensitive sites or critical infrastructure around the country. But also, it bumps it up to the Federal level so that it goes in that shared eGuardian space. I mean, that is significant progress.

Chairman LIEBERMAN. Yes, that is good to hear because Senator Collins mentioned earlier the bill that we put in encouraging the See Something, Say Something approach, which is really an important idea, talking about expanding our forces. Then you are involving everybody. But the natural place that a citizen who sees something and wants to say something will call is the local police department. They are not going to know, generally speaking, how to get to the JTTF or the fusion center. Maybe they will call the FBI, but I doubt it. They will probably dial one of the easy codes that they can dial to get to a dispatcher.

So your dispatchers are trained as you described, just to take that suspicious activity report and send it through the chain of analysis and verification, and then ultimately it will go up to the Federal Government, I assume, if it is a——

Chief LANIER. If there is a counterterrorism nexus, it will go into the shared space. If there is a criminal nexus, it will go in for investigation externally to the law enforcement community. So there is pretty extensive vetting before it is pushed into shared space, but it does—if there is a potential connection to counterterrorism,

it goes into shared space, usually within a short period of time, a couple hours.

Chairman LIEBERMAN. Give me a status report, I suppose, on this question. At various times, we have talked about the fact that if a local police officer stops somebody and is suspicious of them and checks them, goes to the laptop that a lot of them now carry in their cars and checks the name on databases, we know that they will naturally plug through the criminal information database, but it is routine now that they also will plug into terrorism watch lists?

Chief LANIER. That is correct. We get hits back all the time——

Chairman LIEBERMAN. Good.

Chief LANIER [continuing]. Of all three levels on the terror watch list, and notifications are made. The officers are very familiar with it. And in fact, if there is a connection or a hit, there are instructions for the dispatcher and the officer in the computer as to who to call and how to make that call.

Chairman LIEBERMAN. Good. That is great.

Captain Brooks, let me ask you this. You talked about it a little bit. In this time of budgetary stress, there are some people, and we have already heard voices who are going to say—and I want to give you an opportunity on the record to respond to this—well, do we need both JTTFs and fusion centers? We really cannot afford them both, so maybe we should either cut back on or even eliminate the fusion centers. I want to give you an opportunity to respond to that kind of offensive.

Mr. BROOKS. Thank you, and that is a great question. It is one that comes up all the time. JTTFs are an investigative body. They are the FBI, and in partnership with their local law enforcement counterparts, that is the FBI's ability to investigate terror in this country.

Fusion centers play a much different role. They are not only the information sharing hub. The fusion centers are the place where we build a cadre of terrorism liaison officers, where we train not only the 840,000 cops around the country, but more than a million firefighters around the country and the EMS workers and our private sector partners on indicators and warnings and the seven signs of terror. That is where we have the ability to catalog our critical infrastructure, and as Chief Lanier talked about, then be able to analyze incoming suspicious activity reports against the national threat picture and against what we know about our critical infrastructure. It is the ability to share, as you saw in a couple of the examples I gave, between the whole network of fusion centers and then with the FBI.

Our HIDTA, our fusion center, and our threat squad, our JTTF are one entity. We are collocated together.

Chairman LIEBERMAN. Interesting. Is that typical or atypical?

Mr. BROOKS. Is it not typical, but there are a lot of people that have looked at our model.

Chairman LIEBERMAN. Right.

Mr. BROOKS. And so we have the ability to sit eyeball to eyeball, our analysts with the JTTF agents and investigators, as SAR information is coming in. But as often happens, as Chief Lanier mentioned, many times, that SAR information has no nexus to terrorism. It is about drug dealing or gang activity or firearms traf-

ficking, mortgage fraud. I mean, it could be about a variety of things. And so the all crimes approach, as Ambassador McNamara talked about, gives us the ability to take that information and funnel it to the right place, and we know, sir, oftentimes, activity that at first blush appears to be criminal in nature—the Torrance gas station robberies, the smuggling of the cigarettes in North Carolina——

Chairman LIEBERMAN. Right.

Mr. BROOKS [continuing]. The sale of pseudoephedrine in California—that money is funneling back, or that is a precursor to a terrorist act. We cannot really separate crime and terror. We have to knock that wall down. If we are really going to be effective, we have to make sure that we understand that the sharing of information makes communities safe. Our end state is to prevent terrorism, but in my own community, right across the bay from San Francisco where I work, the City of Oakland, they have had 740 shootings to date. That is a city of 400,000. That is terror right there in our own community, and that kind of terror is one that is experienced in big cities and in small towns across the country.

And so I really think when people are concerned about the money spent on fusion centers, we are in tough budget times and we certainly get that. But fusion centers are uniquely situated to do things that JTTFs or no other program can. They can bring together disparate resources. In my center, I have emergency managers, firefighters, EMS workers, public health workers, cops, and analysts, Federal, State, and local, and private sector, and we can bring all of that data together. We can share information on terror, crime, or other threats. We can make sure that the JTTF gets the information they need, but that the DEA and the ATF and the local law enforcement gets the information they need, as well.

Chairman LIEBERMAN. Thanks for that excellent answer. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Captain, I, too, want to thank you for a terrific answer to that question. The Chairman and I have been fighting off efforts by some of our colleagues to do away with fusion centers. There is this argument that they are redundant with the Joint Terrorism Task Forces or that they are ineffective or they are really not playing much of a role, and your answer distinguishing among the various roles was just what we need to counter it. We may send you to see a couple of our colleagues to better educate them about the differences, but thank you because that is exactly the question I was going to ask, as well.

Chief, I want to ask you a question about over-classification of information. We passed a law last year. It started out on the House side, as I mentioned in my opening remarks, with Representative Jane Harman who introduced the Reducing Over-Classification Act. The House bill only applied to the Department of Homeland Security. It was intended to prevent the unnecessary classification of information at a higher level than was warranted. Once it passed the House, Senator Lieberman and I, in my view, improved the bill by expanding it beyond the Department of Homeland Security to cover all Executive Branch agencies, and it became law a year ago this month.

One of the concepts is to encourage greater use of tear-lines so a lower level of classification of a report that is highly classified can be disseminated more widely. Has it made any difference in the past year?

Chief LANIER. Actually, I followed that through and was glad to see it pass, and I have seen a significant difference. The example I gave of the information I was provided during this last threat, and, in fact, the information I was provided during the threat that was uncovered yesterday, or at least the arrest that was revealed yesterday, is a significant difference.

Back in 2004, when preparing for the fall IMF conference here in the District—this is where you have 8,000 world delegates that come here for the IMF-World Bank conference—there was some specific information that was recovered from a computer in Pakistan about surveillance that had been done on the sites, and I was given a briefing that contained little to no information that would help me to put adequate security in place based on what information I had. I was briefed initially 2 months before the event. I was planning the event. I was putting the security plans in place. And it took weeks of arguing to get access to the information. And when I did finally get access to the information, which was completely over-classified, it changed my entire security plan. There were details in there that were critical to how I planned my security and I would have never known it if I relied on what I was briefed.

I do not see that anymore. I actually in this past threat, during the anniversary, was amazed at how open both the FBI and DHS were with sharing the information, and then, also, in the process as the days went on about including me in briefings as the deliberative process went on about what would be released and how it would be released and what updates on the investigation.

So I have seen a significant change here in Washington, DC, and from talking to Chuck Ramsey and major city chiefs, I think, at least in major cities, they are seeing a big difference across the country.

Senator COLLINS. That is great to hear.

Chief LANIER. Thank you for that.

Senator COLLINS. Well, thank you for the feedback. It is nice to know that it has made the kind of difference that we were looking for, so thank you very much.

Mr. Smith, my final question is for you and it has to do with the issue I referenced in my opening remarks, and that is the strange failure of the Administration to appoint a full complement of people to the Privacy and Civil Liberties Oversight Board. Obviously, this board has gone through sort of a difficult time with members resigning in the previous Administration, and I continue to believe that as we expand information sharing, which I think is absolutely critical, that this board is an important check on the process, just to make sure people are considering the privacy implications. So what do you think is the problem?

Mr. SMITH. I agree completely with you, Senator, about the importance of the board. I cannot speak, obviously, for the White House. I do not know exactly why they have had such a problem. To some extent, the confused and unfortunate history of the board may factor into that.

I think two other factors may be involved, and this is speculation on my part. One is that, by statute, the members and the chairman serve a 6-year statutory term. That is a long time to ask somebody to serve——

Senator COLLINS. Good point.

Mr. SMITH [continuing]. Particularly the chairman, and I understand they want the chairman to be full-time.

A second concern may be whether it is adequately funded. I do not know what the current plans for funding are, but I did recently happen to look at the statute and it is pretty modestly funded for an extraordinarily broad set of responsibilities. So perhaps the Committee should look at some aspects of this.

I mean, it would be presumptuous to suggest what you might do, but asking the White House why they have not filled it, I do not believe it is inattention. I do think they want to do it, but there may be some structural problems that perhaps the Committee could look at.

When you contrast that, by the way, with the President's Intelligence Advisory Board——

Senator COLLINS. Right.

Mr. SMITH [continuing]. Which is not subject to Senate confirmation, reports directly to the President, has extraordinarily high-powered people on it, and has an awful lot of influence within the Executive Branch, that may be, frankly, a better model than the one that is currently in statute.

Senator COLLINS. That is a great idea and I think we should look at revamping it. We have written to the Administration repeatedly on this issue without any notable effect, but I think a 6-year term is too long and probably we should be looking at a 3-year term. I personally opposed the move to a full-time chairman. I do not think that is necessary, and I think that makes it difficult to get someone. We might want to have a full-time executive director, but not a full-time chairman.

Ambassador McNamara.

Mr. MCNAMARA. Just a brief interjection. I strongly recommended to the former Administration and to this Administration before I left government that I, as Program Manager, really wanted that privacy board to be alive, well, working, and cooperating with me. It is a necessary place, I feel, for the Program Manager to go to bounce ideas off, to get an independent view. Sometimes you get so wrapped up in the problem that you forget that there are other aspects that have to be taken into account.

I was very disappointed that the good initiative, within 6 months, in fact, had deteriorated, and for all practical purposes, was moribund.

Senator COLLINS. Exactly. Thank you, Mr. Chairman. I think this was an excellent hearing because of the extraordinary witnesses that we have, not to suggest that it would not have been a good hearing without them. [Laughter.]

But I very much appreciate the expertise that you assembled.

Chairman LIEBERMAN. Thanks, Senator Collins. I agree with you totally. It has been very productive. I am going to end up coming away with a good feeling that we have made significant progress in information sharing over the last decade. I think it was you,

Ambassador McNamara, who said that we had built a foundation but we are not finished with what we have to do. In that regard, you have given us, I think, some very timely information and counsel and some suggestions that I promise you the Committee will follow up on to continue to improve the already improved situation.

Chief LANIER. Can I just add one thing I wanted to get on the record before we close?

Chairman LIEBERMAN. Chief, you have the full First Amendment rights. [Laughter.]

Chief LANIER. Thank you. One of the things that is in my testimony, but I did not get a chance to get to it, is still a problem with information sharing, is the D-Block.

Chairman LIEBERMAN. Yes.

Chief LANIER. During the earthquake that happened here in Washington, as you know, just a few weeks ago, literally, there was no phone service for anyone. I was on the street. I was with two other police chiefs in downtown Washington. None of our cell services worked. Using the GETS Card is great. You can get the GETS emergency service up.

Chairman LIEBERMAN. Right.

Chief LANIER. It takes time. I do not think we should have that situation 10 years after 9/11, where you cannot make a phone call when there is a disaster that is unfolding. So any help you could give us on the D-Block would be really important for us.

Chairman LIEBERMAN. Thanks for bringing that up and relating it to this. You cannot share information if you cannot get information. We both are strong supporters of the D-Block auction and the commitment of the D-Block to public safety. There is growing support for it. There still is opposition to the auction from people who would have to pay, but I think we have the majority and we have to find a vehicle to get this through. It almost, believe it or not, got into one of the versions of the debt ceiling extension over the summer. I hope and believe that there will be an attempt to put it into the report of the Joint Special Committee, the so-called supercommittee created by the Budget Control Act. So I am more optimistic than not that we are going to find a way in this session to both have the auction, raise the money, commit the D-Block to public safety, give you some funding to implement that, and then also have some money left over to go toward deficit reduction.

Chief LANIER. Thank you very much. It is very important.

Chairman LIEBERMAN. Thanks very much for your lifetime of service and for your testimony this morning.

We are going to leave the record open for 15 days for any additional questions or statements that Members may have.

With that, the hearing is adjourned.

[Whereupon, at 12:08 p.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11 AND THE ANTHRAX ATTACKS: PROTECTING AGAINST BIOLOGICAL THREATS

TUESDAY, OCTOBER 18, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:04 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Collins, Brown, and Moran.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. Thanks to our really excellent panel of witnesses for coming today to discuss this topic, which is our Nation's record over the past decade in improving our defenses against a biological attack or a pandemic.

Today's hearing is part of our "Ten Years after 9/11" series assessing the status of a number of government homeland security operations that were singled out as inadequate or dysfunctional by the 9/11 Commission. The impetus for our review today, as everyone will remember, actually came a week after the 9/11 attacks, long before there ever was a 9/11 Commission, when our already traumatized Nation was shaken anew by the mailing of anthrax spores to five news media organizations and two U.S. Senators.

All told, five people died from anthrax inhalation. Two were postal workers. And one close to my home was a 94-year-old woman from Connecticut. Twenty-two others were sickened, and thousands—including a lot of Members of Congress and our staffs—took a course of powerful antibiotics to ward off possible infection.

We remember those days well around here because one of the letters was sent to Senator Daschle's office in the Hart Building, where my office was and is located. The building was evacuated and closed for months while HazMat teams scoured the area. We were fortunate that no additional anthrax was found and that no attacks, of course, have occurred since. But that is unlikely to remain the case.

Three years ago, the Graham-Talent Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism concluded that a biological weapon was more likely than any other weapon of mass destruction to be used in an attack against our

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00297 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

country that causes mass casualties. The Commission predicted that such an attack would probably occur somewhere in the world within the 5 years after its report, which was 3 years ago, and concluded then that the Federal Government was not prepared to respond adequately.

Just last week, the Bipartisan WMD Research Center, which was a follow-on to that Graham-Talent WMD Commission, reported that the threat of a bioterror attack remains as strong as ever. We have no specific credible evidence, I want to make clear, that terrorists are now plotting such a specific attack. But they certainly have made it clear in words and action that they aspire to do so, and technological advances, I am afraid, are making it easier, faster, and cheaper to carry out such an attack.

So our question today is: Has the Federal Government developed the tools we need to respond effectively to a bioterror attack or naturally occurring pandemic disease, to develop and disseminate vaccines and antibiotics, and to respond to the medical consequences that would result from such a biological disaster?

Over the past several years and past decade, we have spent billions of dollars on biodefense research; on strengthening first responder capabilities; and on developing new vaccines, biosurveillance systems, and forensic science techniques. Really we have done a lot more than, I would say, the average American knows we have done to protect their security.

These investments, in my opinion, have made us a Nation far more prepared to deal with a biological disaster than we ever have been. Just yesterday, for example, I noticed in the news that the Connecticut Children's Hospital, which is located in Hartford, conducted an exercise to test if it could immunize its employees within a 24-hour period in the event of a virus outbreak or a bioterror attack. This is typical of preparedness at the local level which is going on all over the country and is absolutely key. Communities across the country have significantly improved their disaster planning since 2001.

But it is also clear from the reports that have been issued that we are not prepared for a catastrophic biological incident. We are much better prepared for a smaller WMD biological attack although there, too, are gaps remaining in our capabilities, which I would like to talk about during this hearing.

Since 9/11, Congress has created a remarkable number of new offices to deal with this bioterror threat, so we have not sat back.

The Biomedical Advanced Research Development Authority, established at the Department of Health and Human Services to fund WMD medical countermeasures—that is what products and programs do we have to address the questions: What do you do if there is an outbreak? How do you stop it and protect people? It has helped greatly increase our preparedness by delivering medical countermeasures to the National Strategic Stockpile, which now contains millions of doses of smallpox and anthrax vaccines; post-exposure therapeutics for anthrax, smallpox, and botulism; and some basic radiation treatments. As a result, our ability to treat victims with medical countermeasures has improved dramatically since 2001.

At the Department of Homeland Security, the National Bioforensics Analysis Center studies new bioforensic methods and identifies the DNA of biological agents so that criminal investigators can pinpoint their source.

The Obama Administration is also tightening security at laboratories that use the most dangerous pathogens and those most likely to be capable of being weaponized. I am pleased to note that legislation, which this Committee produced in October 2009, has helped to facilitate this Administration action.

The government has also deployed—and, again, I mention this for the benefit and hopefully the greater sense of security of the public—a network of aerosol sensors called BioWatch in cities around the country that is designed to detect anthrax and other biological agents. New technology is on the horizon that would shorten the amount of time that it takes these sensors to detect a biothreat.

These are significant advances, in my opinion, in our biodefense, but they do not tell the whole story. Last week, the Bipartisan WMD Research Center concluded: "Although [government] efforts have yielded considerable progress over the past decade, the Nation does not yet have adequate bioresponse capability to meet fundamental expectations during a large-scale biological event." And I stress "biologial event."

We still, as far as I can determine, lack a strategy for dispensing vaccines and antibiotics in a mass crisis. We do not have the ability to track the spread of disease in realtime through a community or quickly reclaim contaminated areas to get people back to their homes and critical infrastructure up and running again.

And 10 years after the anthrax attacks of 2001, as far as I can tell, we still do not have a modern anthrax vaccine that is more effective than the one developed in the 1950s. Medical countermeasures for other chemical, biological, radiological, and nuclear threats have also not yet been developed.

Tight budgets now have led to an understaffed medical surge force to respond to a biological attack in communities around the country. In fact, right now discussions are underway in Congress to eliminate funding for programs that coordinate the overall medical response to a bioattack, such as the Metropolitan Medical Response System, and for centers that train public officials in emergency response.

So the Department of Homeland Security, the Department of Health and Human Services, and the FBI, working together and in coordination with State and local governments and the private sector, have an enormous responsibility to continue to work to increase our capability to protect the public from biological attacks. This Committee has been working with those Federal agencies to make sure that they can fulfill that responsibility, and we will continue to work with them in that direction to make sure they can do so in a way that is ever more effective.

So, bottom line, as I look back over 10 years, we have come a long way. Perhaps we will never be as fully protected as we would like to be, but we still have a ways to go. I would like to focus with the witnesses on both elements of that story. What have we done since 2001? And what are the most pressing unmet needs that we

have? So I look forward to the thoughts of this excellent panel of expert witnesses today.

Senator Collins, I really appreciate you coming. I know you are involved in the appropriations bill on the floor, and you are probably not going to be able to be with us very long. But thanks for coming by for an opening statement.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

It has been a decade since the anthrax attacks that left 5 people dead and 17 sickened. It has been just 2 weeks since the operation in Yemen killed Anwar al-Awlaki, who reportedly sought poisons, including cyanide and ricin, to attack the United States.

The new leader of al-Qaeda has a medical background, which raises concerns that he may have an even greater interest in pursuing chemical and biological terrorism.

Since 2001, more than $65 billion in Federal funds have been invested in biodefense, but progress has been difficult to quantify.

With the growth of new technologies and online road maps, terrorist groups may soon be able to threaten nation states with biological weapons. And some countries, like Syria, have never ratified the Biological Weapons Convention.

As the Chairman mentioned, former Senators Graham and Talent issued a report in 2008 on the prevention of WMD proliferation and terrorism. They predicted the use of a weapon of mass destruction, most likely a biological weapon, in a terrorist attack by the year 2013. Just last week, they issued a report card grading improvements in detection and diagnosis capabilities, medical countermeasures availabilities, and communications.

Their report card is troubling. While it does show progress in some areas, they found stagnation on medical management and on the development, approval, and dispensing of medical countermeasures. The Members of this Committee have only to think of our extensive investigation into the difficult time the Administration had in distributing the flu vaccine to respond to the naturally occurring H1N1 outbreak.

The Administration received F's from the Commission in areas such as the attribution of even small-scale events and the environmental cleanup of large-scale incidents. That is not acceptable.

To safeguard our citizens against bioterrorism, we must have the ability to respond effectively after an attack has occurred. But this is no easy matter. We do not yet have adequate bioresponse capabilities to meet fundamental expectations during a large-scale attack. The WMD Prevention and Preparedness Act that Senator Lieberman and I introduced in 2009 would have required the establishment of a detailed plan for preventing and responding to such an attack.

A biological attack is especially worrisome because we likely would not immediately know that we had been attacked. That is why I remain concerned about the effectiveness of the BioWatch Program. Secretary Janet Napolitano has touted this nationwide environmental monitoring system designed to detect the intentional release of aerosolized biological agents. But according to the

GAO, a threat agent may not be identified until more than a day after its release.

While the next generation of BioWatch technology could bring this down to just 4 hours, we are not yet certain that this technology will be viable.

In addition to the technological upgrades, better coordination between DHS and HHS is necessary to enhance our ability to identify a threat agent quickly and to increase the speed and reliability of attribution so that we can help prevent follow-on attacks.

Ultimately, our best hope of detecting and containing an attack is the low-tech, unglamorous, but critically important system of intelligence combined with a robust public health surveillance network. This still remains the most effective system, and we must be careful not to look for technological magic bullets to relieve us of the duty to maintain and strengthen our public health surveillance infrastructure.

The Graham-Talent Commission also found serious flaws in the security of biological labs in this country. A GAO report in 2009, which I requested, reported alarming deficiencies in basic perimeter security at facilities that house the world's most dangerous pathogens, like the Ebola and smallpox viruses. GAO also found that laboratory regulation "for the most part relies on self-policing."

I was pleased to hear the Chairman say that the Administration has taken some steps to improve security at these labs. I look forward to hearing what those are.

While security controls must be improved within our own country, global security problems are even more daunting. I mentioned Syria earlier, but the crossroads of terrorism and proliferation, biology, and technology, in volatile countries such as Pakistan are also troublesome.

A multitude of Federal agencies—DHS, EPA, HHS, CDC, USDA, and the FBI, among others—all have some responsibilities for bioterrorism. I will tell you, it concerns me that so many different Federal entities could be scrambling to respond during and after an attack. And that is, of course, in addition to State and local health officials and first responders that are a critical part of the system as well.

Yet the Executive Branch does not have one agency or one official that is the clearly designated leader on all elements of biodefense, especially the coordination and dissemination to both law enforcement and public health stakeholders of critical information.

This appears to me to be a major gap in our prevention and response capability. If we cannot tell our health providers what to look for when there is a potential threat, we cannot properly trigger the public health surveillance system that is our best hope for early detection, containment, and response.

We need a leader who can direct the response and eliminate overlap or redundancy. This official should also have the ability to coordinate across Federal agencies and harness the assets and expertise of State and local governments, first responders, and the private sector.

Although, as the Chairman has indicated, I am going to have to leave early from this hearing to manage a bill on the floor, I can

assure the witnesses that I will follow with great interest your testimony, and I look forward to reading the questions and answers.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins, and if you are not able to return, as I presume you will not because you are managing the bill, I am going to make sure to ask the witnesses to respond particularly to your last couple of questions about coordination among the many Federal agencies involved here.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thank you.

Our first witness is Dr. Tara O'Toole. Dr. O'Toole was before us in an earlier incarnation as a noted biodefense expert and founder, in fact, of the Center for Biosecurity at the University of Pittsburgh Medical Center. It is a pleasure to welcome you back as the Under Secretary for Science and Technology in the Department of Homeland Security and to welcome your testimony at this time.

TESTIMONY OF HON. TARA J. O'TOOLE,[1] UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, U.S. DEPARTMENT OF HOMELAND SECURITY

Dr. O'TOOLE. Thank you, Mr. Chairman, Senator Collins, and Senator Moran. As you have both already eloquently stated, there really has been a lot of significant cumulative progress in many of the areas of this complex landscape of biodefense over the past decade, and I will highlight some of the S&T Directorate's contributions in understanding the threat, detection and characterization, response, recovery and decontamination, bioforensics, and last but not least, defense against agro-bioterrorism, which is very important even though we have not experienced such an event before.

Senator Collins, as you both noted, at the Federal level biodefense is an intensely interagency activity. I think the subject represents such irreducible complexity that at some level there is no help for learning how to coordinate across multiple Federal agencies and, indeed, as you said, State and local governments, the private sector of health care, and public health.

In particular, in austere budget environments I think collaboration among the Federal agencies is going to become even more imperative as we try to conserve resources and make sure our priorities are correct.

What you see before you today is the beginning of an actual community of biodefense experts in the government, which we certainly did not have, at least not as robustly as we do today, in 2001. I would caution you, however, that some of the budget cuts being contemplated will do great damage to that community, and if people do not see career paths in biosecurity, then this complex melange of technical subjects may suffer, and so will the Federal Government's expertise in this area in time to come.

And, finally, I just want to commend this Committee for your continuing interest in this topic. This Committee is really one of the only places in Congress that the entire landscape of biodefense is overseen and examined, so this, I think, is a very important hearing.

[1] The prepared statement of Dr. O'Toole appears in the Appendix on page 1150.

First of all, what is different since 2001? We have a much better understanding of the risks associated with specific biothreat agents under particular scenarios. Part of this understanding comes from S&T's Biothreat Risk Assessment, which is done biannually. We have done three of these major probablistic risk assessments, which are strategic assessments, models, which identify and prioritize the relative risk, as I say, of different agents and serve as the starting point for biodefense priorities and investment decisions.

The BTRA, as it is known, also identifies knowledge gaps that are then pursued by the National Biothreat Center at Fort Detrick and provides a systematic, science-based framework for asking "what if" questions. What if it was a lot easier to get hold of this agent? What would that do to the risk? And so forth.

Every other year when we are not doing this elaborate risk assessment, we conduct what are called tailored assessments which focus on more detailed evaluation and hypothesis testing. For example, what is the impact on producing agents given a range of judgments from the intelligence community about how easy that might be to accomplish?

We are also in S&T pursuing detailed and empirical risk studies on the effects of releasing a biological agent or a chemical agent in metro systems. We have done this in Boston and in Washington, using both biological and chemical simulants to understand what would happen to these structures under attack and how to recover them quickly.

Chairman LIEBERMAN. What kind of metro systems are you referring to?

Dr. O'TOOLE. The Massachusett Bay Transportation Authority in Boston and the Washington Metro, the oldest and the newest.

Chairman LIEBERMAN. Actual metro transportation.

Dr. O'TOOLE. Exactly. Subways, as we call them in Boston.

In the category of detection and characterization, as you noted, in 2001, once it was recognized that letters containing anthrax had been mailed to media outlets and Congress, there was an avalanche of reports of suspicious powders causing thousands of first responder requests and a tsunami of samples being sent to State labs for analysis. The response was very disorganized, confused. It engendered a lot of alarming speculation and repeated calls and responses that ranged from building evacuations, to stripping people who had been in the buildings and washing them down, and to closing buildings for years at a time.

I think the reaction would be much different today. S&T has led an interagency working group with the same alphabet—CDC, FBI, HHS, and NIST—to create the Standard Field Protocol for Rapid Resolution of Suspicious Powders. This guidance basically walks first responders through how to deal with a visible powder they suspect of being a bioagent, protecting themselves and also yielding a sampling strategy that would stand up to reliable testing and prosecution if necessary. These are also much more effective and efficient procedures. They are already being used by the FBI in several States, and they are now being incorporated into first responder training curricula.

We are also in S&T evaluating the ability of commercially available technology which would rapidly test powders in the field to be reliable. These technologies were available in 2001 and were not reliable. There were a lot of false positives which caused a lot of mayhem.

Because S&T and others have developed reliable standards for doing assays of microbiological agents, we can now effectively evaluate these commercial options and tell first responders what works and what does not.

As Senator Collins says, the Lab Response Network is critically important to our biodefense. This is a State-sponsored network of public health labs which are the ones that carry out the assays that would come to them via the first responders. They, too, are much more organized and capable than they were in 2001. They, too, are using standardized assays developed by S&T and the interagency, and we are working on technologies that would allow them to surge more effectively if they were suddenly, again, to encounter large swaths of tests.

I will point out, however, that the robustness of this important leg of our response is also in peril. Since 2008, we have lost about 50,000 public health staff in the State and local public health agencies due to economic pressures.

I will mention a final technology in detection and characterization category that S&T is working on. This is an outcome of our work on metro studies. We called it "Detect to Protect." We are concerned that we need to be able to respond faster to detection, so we are looking at a two-tiered system, first, of very fast detectors that would automatically trigger low-impact action, such as turning off HVAC systems, and at the same time would trigger a slower but more reliable detector that would then confirm whether or not this was a true positive.

We are also working on many other things, including advanced diagnostics. We have done a lot of work in recovery and decontamination. We do have initial guidance out there for how we would do that rapidly. I would point out that decontamination is really an issue mostly with anthrax, which is especially hearty. It may not be an issue with other bioagents, at least not in the long term. And DHS along with other agencies, in particular DTRA, are now conducting the aerosolization studies at Dugway Proving Ground to find out exactly whether or not and to what extent anthrax would come back up into the air and pose a risk to health after an attack.

We have made great progress in bioforensics, which is one aspect of attribution. I think this is an area where the WMD report card was a little bit harsh. I would be happy to talk about that. But NBAF at Fort Detrick is an enormous national capability that we are very proud of.

And, finally, agrodefense is also moving forward thanks to great work at the Plum Island Disease Center off the coast of Long Island. We are very close and, in fact, are doing field trials of a new foot-and-mouth disease vaccine, which would allow us to distinguish animals who were infected from a disease versus those who were vaccinated. And DHS is very committed to building the National BioAgro Facility in Manhattan, Kansas, a BSL-4 facility

which Secretary Napolitano and I believe is essential for U.S. agrodefense. That is problematic in the fiscal year 2012 budget, and I would be pleased to take questions on that during the question period.

Thank you very much.

Chairman LIEBERMAN. Thanks, Secretary O'Toole, for that excellent beginning. I cannot control myself from asking whether there is a benign form of the foot-and-mouth vaccine that you will have available to Members of Congress. [Laughter.]

Dr. O'TOOLE. Given the budget, Senator, we would be——

Chairman LIEBERMAN. I apologize, really. But thank you for laughing quietly.

Our next witness is Hon. Alexander Garza, Assistant Secretary for Health Affairs and the Chief Medical Officer of the Department of Homeland Security. Dr. Garza prior to coming to this position was involved in many aspects of practice, including serving in the U.S. military in battlefield circumstances with great honor and effect. He heads the biodefense strategy and planning effort at Homeland Security and runs operational components such as the biological surveillance system I mentioned, BioWatch. So we are very glad to have you back, and please proceed with your testimony.

TESTIMONY OF HON. ALEXANDER G. GARZA,[1] ASSISTANT SECRETARY FOR HEALTH AFFAIRS AND CHIEF MEDICAL OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Dr. GARZA. Thank you, sir. Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, thank you for inviting me to testify before you today. Secretary Napolitano, in submitting the 2011 Progress Report, highlighted a number of activities that DHS has instituted to prepare for and protect against biological attacks. The Office of Health Affairs works on several of these efforts, so I welcome the opportunity to discuss these with you.

I am pleased as well to testify with my counterparts here from the FBI, HHS ASPR, and the Science and Technology Directorate. As was mentioned before, biodefense requires a multidimensional approach if we are to protect the American people, and we very much value the partnerships with these and other Federal agencies.

The Committee is also very familiar with OHA's role and responsibilities. We are the principal medical and health authority for DHS, including acts of terrorism, and are the legislative coordinator for biodefense within the Department. These are responsibilities that I take very seriously as our mission is imperative to the overall mission of homeland security.

As has been mentioned already, the risk of a biological agent being used as a weapon against the United States is both real and concerning. Just last week, the Bipartisan WMD Terrorism Research Center released its 2011 bioresponse report card stating that the threat of biological attack was real and growing.

[1] The prepared statement of Dr. Garza appears in the Appendix on page 1161.

Furthermore, rapid advances in biotechnology have lowered the potential barriers once thought to inhibit would-be bioterrorists. The Amerithrax incident of 10 years ago, although significant, was a small-scale attack with limited casualties. It nonetheless showed that one does not necessarily need a weapon of mass destruction but only a weapon of mass disruption to effect severe consequences, and our adversaries have learned from this model.

The Department has made great strides in protecting and preparing the Nation to respond to biological attacks since this incident. We have improved our ability to detect biological agents, mitigate their effects, speed our recovery, and, most importantly, to save lives. I will discuss our initiatives that are instrumental to biodefense for the Nation, including BioWatch, biosurveillance, and our planning and exercise efforts.

One of DHS's most significant contributions in biodefense is in early detection. The prompt identification of a bioattack accelerates the detect, decide, deliver, and dispense sequence. Put another way, it buys time, and time saves lives.

Now in its ninth year, OHA's BioWatch program is a federally managed, locally operated nationwide environmental surveillance system designed to detect biological agents. BioWatch is strategically deployed to more than 30 high-risk metropolitan areas and at national special security events such as the upcoming APEC summit.

However, BioWatch is much more than a machine. BioWatch has evolved to become a robust network of Federal, State, and local individuals that together form the nexus of decisionmakers in the event of a biological attack.

In 2010, DHS began testing and evaluating the next generation of biodetection systems, which we call Generation-3, or Gen-3. The Gen-3 program's goals are to decrease the time to detection from 4 to 6 hours, increase our population coverage, and provide greater cost-effectiveness all without losing any accuracy. We are currently in the process of a rigorous and well-controlled testing and evaluation program validating this technology.

Early detection through BioWatch is but one element of an overall biosurveillance and situational awareness system. OHA also manages the National Biosurveillance Integration System, a consortium of Federal partners established to detect and monitor biological events of national concern.

DHS has developed and continues to refine an integrated, multidisciplinary, common biosurveillance capability to provide the Federal Government, State, and local partners with information and assessments of potential and unfolding biological events.

Furthermore, understanding that all events are local, we work directly with State and local public health, emergency management, and emergency medical services leaders to develop response capabilities for health security threats, including biological threats.

For example, we are expanding local public health participation in the national network of fusion centers, and OHA together with FEMA conducted a series of anthrax response exercises in each of the 10 FEMA regions. These exercises were designed to help coordinate roles, responsibilities, and critical response actions following a wide-area anthrax attack.

Last, OHA coordinates routinely with our Federal partners, including those at this hearing, on various medical countermeasure issues. These efforts include the interagency development of a Federal rapid response capacity and the DHS effort to stockpile medical countermeasures for our personnel, which my office has led.

As demonstrated by these multiple examples, DHS has made substantial investments and improvements since the 2001 anthrax attack, and we are much better prepared than we were a decade ago. There still, however, remains much work to do in biodefense going forward.

I thank you for your time and look forward to answering whatever questions you may have. Thank you, sir.

Chairman LIEBERMAN. Thank you, Dr. Garza, for that excellent testimony.

Next we have Dr. Nicole Lurie, who we are again glad to welcome back—we have four doctors on this panel, and it is reassuring. She is the Assistant Secretary for Preparedness and Response at the Department of Health and Human Services. Dr. Lurie heads the biodefense strategy and planning efforts at HHS and in that regard oversees efforts to develop vaccines and therapeutics under the Project BioShield in BARDA. So thank you for your work, and we look forward to your testimony now.

TESTIMONY OF HON. NICOLE LURIE,[1] ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Dr. LURIE. Thank you. Mr. Chairman, Ranking Member Collins, and Senator Moran, as you heard, I am Dr. Nicole Lurie. I am the Assistant Secretary for Preparedness and Response, and I am pleased to talk with you about our Nation's public health preparedness for a biological event.

As we all know, 10 years ago, on the heels of the World Trade Center attacks, we all dealt with the anthrax letters, which we have talked about this morning. While we were ill prepared at the time to face those attacks, today I am pleased to tell you that our public health preparedness has made steady and really significant progress. With each emergency, from hurricanes and tornadoes to a pandemic and an oil spill, we have continually improved in our planning and our operations. We now have strategies in place to coordinate our efforts and have built truly all-hazards capabilities from the local to the Federal level to ensure that our responses are flexible and can save lives.

One area of progress is in the medical countermeasures enterprise, beginning with surveillance running all the way through to dispensing and evaluating a countermeasure. Yet I will be the first one to tell you that, despite the gains, progress has not been fast enough.

In December 2009, Secretary Sebelius requested a review of the medical countermeasures enterprise to ensure that the Nation really has a forward-looking, 21st Century system. We have made many improvements in response to that review, including strength-

[1] The prepared statement of Dr. Lurie appears in the Appendix on page 1167.

ening surveillance, laboratories, and countermeasure distribution plans.

Critical to the success of the whole Public Health Emergency Medical Countermeasure Enterprise is an integrated approach with a formal governance structure. And you should know that this includes all of the components of HHS plus DHS, VA, DOD, USDA. So it is truly an interagency effort. And that all parts now of HHS, CDC, FDA, NIH, and the Biomedical Advanced Research and Development Authority work together with companies from the outset of a contract rather than at the end of the pipeline.

In this arena, active partnerships with industry have become really critical, and we have created new opportunities to communicate our priorities and help companies, especially new ones, learn how to work more effectively with us.

We have also strengthened our internal processes, making the government an easier partner to work with, and I am pleased to report, for example, that we have decreased the time it takes to announce, review, and award new contracts for our broad agency announcements by almost 25 percent in the last year, to under 6 months.

The medical countermeasure review also prioritizes regulatory science at FDA and proposes innovative partnerships with industry to support promising new companies and ideas.

Thanks to the BioShield special reserve fund, we have procured and stockpiled more critical life-saving countermeasures than at any time in our Nation's history, including for smallpox, anthrax, botulism, and radiological and nuclear threats, as you mentioned. Through work in BARDA, we now have a pipeline of new products, including over 80 candidate products that, if successful, have the potential to transition to the stockpile. And we continue to make progress in preparedness for the next influenza pandemic.

Through a long-term partnership with Novartis, for example, the first U.S. cell-based influenza manufacturing plant will become operational in the next couple of weeks. This plant will expand significantly our domestic surge capacity for a pandemic vaccine and could also make vaccines for other novel emerging pathogens in an emergency.

Chairman LIEBERMAN. Just tell us a little more about that, because our Committee was so focused on that during the H1N1 hearings we held. Tell us where it is going to be. This will be the first inside the United States now.

Dr. LURIE. This is the first cell-based facility inside the United States. It is in Holly Springs, North Carolina, and it has been a long-term partnership with Novartis.

Chairman LIEBERMAN. Right.

Dr. LURIE. Then, in addition, we are reviewing applications now for the Centers for Advanced Development and Manufacturing called for in the Secretary's medical countermeasure review which will provide core services to companies and then additional surge manufacturing capacity. I do not know where those will be yet because that is still in process.

Chairman LIEBERMAN. Well, that is really good to hear. I remember during the outbreak that we were very concerned that we were dependent on foreign manufacturers, and they would naturally feel

pressure to give first to their local populations, and quite understandably. So that is very significant. I am glad to hear that.

Dr. LURIE. Yes. Thanks. I think the progress has really been remarkable, and I congratulate both Congress for funding and our team and our partners for really pulling it off.

Yet, as we all know from the WMD Terrorism Research Center report card, while we have made important progress—and that is some of it—our preparedness is not yet sufficient. In particular, they noted that the medical countermeasures enterprise lacks sufficient and sustained funding. The reauthorization of the Pandemic and All-Hazards Preparedness Act is one opportunity to provide some new authorities and resources called for in that report.

On the response side, we are using new technologies, including electronic medical records to match demand with need, geographic information systems to identify the needs of affected populations and available resources, and social media to communicate and observe developing health trends.

We have also made impressive strides in our Nation, in our core State, and local public health capabilities. So there was a time in the not too distant past, in fact, when you and I had a chance to speak, when getting Internet access for a local health department was a challenge, and blast fax was a breakthrough technology. We can all laugh about it now. It was not very long ago.

Two-thousand-eleven has seen a number of natural disasters that were ably managed by our State and local partners with limited or no Federal assistance, and we have heard repeatedly from them that this would not have been possible 10 years ago.

Two critical tools that underpin State and local response are the Hospital Preparedness Program and the Public Health Emergency Preparedness Program, which are being aligned for greater efficiency. However, without continued support and funding for our public health and medical systems, the infrastructure will degrade. In fact, as you heard from Dr. O'Toole, we are seeing this already in this loss of almost 50,000 jobs. My fear is that as State and local capacity diminishes, we will see an increase once again in the call for Federal assistance, but, furthermore, this really puts our Nation's response capability and community recovery at risk. Sustaining our community-based response capabilities has to remain a top priority.

Ultimately, all of our investments and efforts have the same goal: Building a resilient Nation and saving lives when a disaster does occur. We have made great strides in the last decade. I am very proud of what we have accomplished in the last 2½ years, but in truth, we have miles to go before we sleep.

Thank you for the opportunity, and I am happy to answer any questions you may have.

Chairman LIEBERMAN. Thanks very much, Dr. Lurie.

Last on this panel is Dr. Vahid Majidi, who is the Assistant Director at the FBI in charge of the Weapons of Mass Destruction Directorate. It says a lot that Dr. Majidi, who has a very distinguished background as a chemist and worked at the National Laboratories, now finds himself at the FBI where he is responsible for investigating suspected cases of WMD terrorism and proliferation.

So I am very glad you are here, and please proceed with your testimony.

TESTIMONY OF VAHID MAJIDI, PH.D.,[1] ASSISTANT DIRECTOR, WEAPONS OF MASS DESTRUCTION DIRECTORATE, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. MAJIDI. Thank you, sir. Good morning. It is my pleasure to discuss what the FBI has done over the last 10 years and what we are doing to protect the United States against bioterrorism threats.

The FBI's number one priority is to protect the United States from terrorist attacks, and within that priority, the use of weapons of mass destruction is simply unacceptable to us. In fact, to clearly demonstrate our commitment and to ensure that we rigorously address WMD issues, the FBI established a Weapons of Mass Destruction Directorate in 2006. The Directorate consolidates WMD investigations and prevention efforts, creating a unique combination of law enforcement authorities, intelligence and analysis capabilities, and technical subject matter expertise focused on chemical, biological, radiological, nuclear, and explosive matters. My Directorate's primary mission is prevention of WMD terrorism and proliferation.

The FBI has the responsibility to investigate WMD threats, and often we have to use our strong response capabilities to collect evidence in contaminated areas, disarm hazardous devices, and provide command and control support for critical incidents.

Threats are identified through products from the U.S. intelligence community, which includes FBI's collections efforts, and leads are provided through the local law enforcement community as well. Domestic and international terrorist groups, such as al-Qaeda and its affiliates, have shown unwavering interest in using biological agents and toxins. It is not unusual for these groups to openly seek scientists to join their ranks and support their cause.

The FBI addresses bioterrorism threats by identifying points of vulnerability for biological agents acquisitions, weapons development, and ultimately the execution phase. This systematic approach allows for resources prioritization in light of potential gaps in our biosecurity program. We have a well-defined framework to design and implement countermeasures focusing on our outreach and indicators.

There are challenges mounting an effective response to an act of bioterrorism. These events may go undetected for a long period of time until victims seek medical treatment or other key evidences are discovered. As such, the FBI and CDC developed the Joint Criminal and Epidemiological Investigations. This is an interactive training program to improve public health and law enforcement efforts to jointly identify and investigate intentional or naturally occurring threats.

As you mentioned earlier, a recent bioresponse report card published by the Bipartisan WMD Research Center provides an overall negative view of U.S. Government accomplishments in bioterror readiness. Nonetheless, they do highlight that CDC and FBI have made considerable progress in building partnerships between pub-

[1] The prepared statement of Mr. Majidi appears in the Appendix on page 1186.

lic health and law enforcement that will significantly improve cooperation during investigations.

I must emphasize that FBI's program in combating bioterrorism is based on prevention concepts, which is much more expansive than leading-edge investigative protocols, advanced traditional forensics, and microbial forensics familiar to all. Amongst the pantheon of activities centered on WMD issues, the FBI is keenly focused on safeguarding biological organisms and the security of individuals with access to these materials. We developed the Biological Sciences and Academic Biosecurity Workshop Initiative to build partnerships between the FBI and academic research communities. This initiative improves situational awareness for all participants and develops a mechanism to report suspicious activities to prevent emerging national security threats.

As you are aware, the FBI is a Federal partner in the Select Agent Program with HHS and USDA, and this program is designed to safeguard entities that store or conduct research with biological select agents and toxins. The FBI supports this program by properly vetting individuals prior to access against any of the 10 prohibitors defined in the USA PATRIOT Act and 18 U.S.C. 175(b).

The FBI has at least one highly trained special agent in each of our 56 field offices who manages and addresses WMD threats and events. These special agents are known as WMD coordinators. The FBI laboratory has developed an extensive protocol and strong national relationship with U.S. Government components, including DHS's National Bioforensic Analysis Center, to deal with WMD evidence. Biologically contaminated evidence is evaluated by the Laboratory Response Network established by FBI, CDC, and associated public health laboratories.

Additionally, the FBI created the Hazardous Evidence Analysis Team, a cadre of highly trained forensic examiners who are capable of safely performing traditional forensic analysis on contaminated evidence in our partner laboratories.

Advancements in science and technology have led to significant progress in synthetic biology. The FBI has established a synthetic biology initiative, a proactive approach to mitigate current and over-the-horizon risks posed by exploitation of advancements in this arena. In a partnership with private industry, we have implemented the Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA. This framework codifies a notification process for DNA sequence providers to contact their local WMD coordinator, which I mentioned earlier, when encountering alarming orders.

Moreover, growing public interest in biological science has led to the development of an amateur biology movement. In this community, science and biotechnology is pursued at home or shared meeting places. The FBI has developed a partnership with the amateur biology community to garner collaborations in preventing, detecting, and responding to potentially nefarious incidents. In short, the FBI is dedicated to protecting our Nation and will continue to collaborate with the U.S. Government and scientific community to proactively address new biological threats on the horizon.

Since the establishment of the Weapons of Mass Destruction Directorate, the FBI has successfully managed hundreds of cases in-

volving biological substances and suspicious powders, leading to numerous convictions and lengthy sentences.

Thank you for your time. I look forward to answering your questions.

Chairman LIEBERMAN. Thanks, Doctor.

We will do 7-minute rounds of questions. Senator Moran is here, and Senator Brown said he would try to come back from another committee hearing.

Dr. O'Toole, let me begin with you, and thank you for the work that Science and Technology has done. I want to ask you to talk to us a little more about the strategic risk assessments that you have carried out, and tell us in a little more detail what they show.

Dr. O'TOOLE. These risk assessments are models. They are computer models based upon the best scientific data and the judgments of professionals—including intelligence community professionals and law enforcement experts—that we can find. "All models are run, some are useful" is the rule of thumb, and the same goes for BTRA.

I would be happy to tell you how the agents themselves rank and what scenarios we are most worried about in a classified session. I cannot talk about that now. But what the models produce is information of that sort: What agents really could create a mass casualty situation and under what conditions.

It allows you to say, well, if I change this variable, so, for example, if I made it impossible to get a bioagent such as smallpox, then that scenario goes away or is greatly mitigated.

What happens if you could have medical countermeasures against a certain agent under reasonable expectations of distribution and efficacy and so forth? How many lives would you save?

So you can ask questions of these models and probe them, and then take the uncertainties that you uncover and actually investigate those in laboratories, which we do, and back, in Frederick, Maryland.

They act in practice as the starting point for decisions about which biothreat agents do we need to be most worried about.

Chairman LIEBERMAN. That is the important point. This is a unique function that you are carrying out.

Dr. O'TOOLE. Yes.

Chairman LIEBERMAN. And the results of these strategic risk assessments are then shared across the board in our government, and presumably State, local government, and the private sector, in terms of how the attacks are most likely to come and, therefore, I presume, how we should work to develop countermeasures.

Dr. O'TOOLE. Yes. The last is particularly important. The bioagents of greatest concerns are then further studied in detail. We validate the original assumptions. We make sure we have up-to-date intelligence. And then the results of that second analysis are forwarded to HHS, where they consider them in their own framework in terms of public health impacts.

First of all, the design of the Biological Terrorism Risk Assessment is an interagency process, and the results are disseminated through the interagency and find their way into an array of activities, from what kind of exercise are we going to pursue in terms

of decontamination to what countermeasures are we going to pursue to a myriad of other things.

Chairman LIEBERMAN. Let me go back to the baseline. I obviously respect and support your conclusion that you do not want to describe this in detail in a public setting. But I take it, generally speaking, that the result of the strategic risk assessment is that you continue to consider the threat of a bioterrorist attack to be real. In other words, there is a second look here around the tenth anniversary of 9/11 where some people are beginning to say that in general, not just in terms of bioterrorism, we have overreacted over the last 10 years.

Dr. O'TOOLE. Can I address that directly?

Chairman LIEBERMAN. That is what I would like you to do.

Dr. O'TOOLE. The biothreat is real, as Dr. Majidi said. We know our adversaries are pursuing biological weapons. The potency and the accessibility of these weapons, as you said, will increase as the bioscience revolution proceeds.

Just as an example of how fast we are learning how to manipulate biological organisms, in the 1990s it took a decade and $1 billion to decode the human genome. We could now do that for $1,000 in about a week. And that is only one technique.

At the same time, this progress is happening globally. It is not owned by the U.S. Government or any government. It is being pursued avidly by huge amounts of capital in biopharma, biofuels, and all kinds of places, including amateur biologists and kids who are interested in extracting DNA for fun, similar to the computer revolution that began the IT industry. So this is going to proceed apace, and the appeal of asymmetric weapons is not going to go away either among terrorist groups or among sovereign states, I would suggest. This threat is not going to go away. It is going to grow.

Chairman LIEBERMAN. Yes. Dr. Majidi, you agree with that, I assume. For instance, the Graham-Talent Commission, as you probably know, said that they considered a biological attack to be the most likely of the various forms of weapons of mass destruction attack because of the relative ease of developing biological agents and moving them into the country. Do you agree?

Mr. MAJIDI. Yes, that is correct, sir. In fact, if you look at a historical perspective as well as the current case trend, biological cases tend to be the largest portion of our WMD cases that we investigate. Many of them tend to be hoaxes, but, nonetheless, the cases that have real material involved in them tend to be biologically centered.

Chairman LIEBERMAN. Yes, I mean, I can tell you that we have a warning system now in the Capitol, usually on our BlackBerrys or cell phones, and there is actually a remarkable number of occasions where the Capitol Police are called to investigate some kind of substance that they do not identify. I think every one of them since 2001 has turned out to be benign, but that is not always going to be the case.

I think it is clear from your testimony that—Dr. Garza or Dr. Lurie, do you want to add anything about the reality of the threat?

Dr. GARZA. I would concur with both of my partners up here. Dr. O'Toole hit on this earlier. There is such a thing as the curve on how quickly biotechnology is growing, and as I mentioned in my

opening statement, this is very concerning. And she made the analogy to computer technology. There is a law in computing called Moore's law where you increase the capacity of your capacitor and the price decreases. Well, the curve for biotechnology is much steeper than Moore's law, and so that barrier that a would-be bioterrorist would have in being able to develop a biological weapon is becoming much easier than it was in the past.

Chairman LIEBERMAN. Dr. Lurie.

Dr. LURIE. Nothing really to add. I would say that for some years I participated as a judge in a contest for high school students who did epidemiology projects. What they did was remarkable and, in fact, sometimes much more sophisticated than many of the other modelers I know.

I think if we were to have such a kind of contest now in the amateur biology sphere, we would be pretty terrified with what they would come up with.

Chairman LIEBERMAN. That is sufficient warning in itself.

I want to go back very briefly, Dr. O'Toole. Obviously, intelligence in the war we are in with the terrorists is more critical than it has ever been in any other war because of the nature of the enemy not striking in any conventional way and also not hesitating—in fact, focusing on civilian populations. So I take it that the intelligence community is fully and directly involved certainly in the strategic risk assessments that your Directorate is doing.

Dr. O'TOOLE. Yes, they are, more and more actually, and the intelligence community itself is rethinking its own approach to the biothreat and putting new emphasis on collection techniques and so forth.

I would urge all Members of Congress to get a classified briefing on the biothreat from the intelligence community. I think that would be very helpful to biosecurity.

Chairman LIEBERMAN. That is a good idea, and I am going to ask Senator Collins, but it might be good for our Committee to begin that and do that in a classified setting.

Let me ask you one more question, and then I am going to yield to Senator Akaka, who I welcome here this morning, and this picks up in a way from Senator Collins' last statement in her opening statement, which is here are four different agencies—well, three with two from DHS—represented and a lot of other agencies clearly involved. Who is in charge? In other words, who is coordinating the efforts of the various departments of the Federal Government involved in both trying to prevent and respond to a biodisaster? Let me begin with that. Dr. O'Toole, do you want to start?

Dr. O'TOOLE. Well, I would have to ask, in charge of what? I understand the longing for a strong leader, somebody who can take decisive action in a crisis, and there is an argument for that. I do think that biosecurity is so complex and involves equities from so many agencies that a coordinator in the White House may be of some use, but I think the question is to some extent a red herring.

In a catastrophic attack, the President is going to be in charge in about 30 seconds.

Chairman LIEBERMAN. That is what I was going to ask. Who is in charge in a crisis? Is there somebody within the White House

who will take the key role in coordinating your effort and advising the President——

Dr. O'TOOLE. Yes, I mean, I think that would be within the National Security staff, either John Brennan or his Deputy, Heidi Avery.

Chairman LIEBERMAN. Right.

Dr. O'TOOLE. But we would all have roles to play very intensely. The interagency approach brings strengths as well as liabilities, and as we saw in 2001 and during the flu pandemic, you need a lot of very detailed, specialized knowledge to have an informed, coherent response to these kinds of events. And we are going to have more and more of them in this society, like Deepwater, like Fukushima. We are not going to be able to predict in advance exactly what constellation of experts we need. We need to have an agile capacity to assemble and reassemble and restructure the capacities of the U.S. Government as needed. That is what we have to learn how to do, and we have to get very efficient at that.

Chairman LIEBERMAN. Maybe I will turn to you, Dr. Lurie. What assurance can we give the public, particularly at this time of tremendous budgetary stress, that there is not a redundancy that is necessary, in other words, that there is not an overlap of public investment because of the many agencies involved in the whole field of preparing for, preventing, and responding to bioterrorism?

Dr. LURIE. Thank you for that. This is an area where I actually feel quite comfortable. I think the governance structure for the countermeasures enterprise is very robust. As I testified, it includes high-level membership from across the interagency. So Dr. O'Toole and Dr. Garza both sit on the PHEMCE steering committee, as do others. We have pretty full visibility into what people are working on and developing, whether it is in different HHS components, whether it is in DOD, whether it is in DHS.

The good part is that we all share expertise and problem-solve around it. We look and say, well, if you are doing X, I need to do Y instead. Or for example, in the case of FDA, how can FDA be at the table earlier with a DOD issue?

So the coordination I think has really grown tremendously over the past couple years and is quite robust. So going back to your first question to Dr. O'Toole, we learn from DHS and get information from DHS about which agents are the threat agents. We do our own public health assessment of how those are likely to make people sick and how many people are likely to either get sick or die. We look at the kinds of products that we need to make to counteract those. And with that, we work across the whole interagency, so we want to know how would a product be used before we even go ahead and make it. Does that make sense? Is it usable? Is it needed? How would it be deployed in the field, for example?

In this space, I actually feel quite comfortable that we have worked very hard to wring redundancy out of the system. In our Centers for Advanced Development, for example, DOD has sat at the table with us, helped put the RFP together, will help provide core funding for it. Again, tremendous opportunities exist for coordination and collaboration that we have taken full advantage of.

I want to go back to your question for a minute also to Dr. O'Toole about this, the sort of "who is in charge" piece, because I

think, as she said, this capabilities-based piece is really important, and we have now a number of structures for governance and coordination across all of us. But I should also point out that at the end of the day, with each of the emergencies that we have faced, whether it was pandemic, whether it was Deepwater, whether it was the effects of the Fukushima crisis, we all sat together in the situation room, led by National Security Council staff, and worked it out, worked through plans and operational responses. And because we work so closely together now day to day on all of these other issues, that has actually been really easy. It is not like you have needed to corral people to sit them down at the table and make them talk to each other. We do that all the time.

Chairman LIEBERMAN. I am going to leave it at that now, but I think your answer, both of your answers, says that you are working together regularly and that the person in charge is in the National Security Council, probably Mr. Brennan or his Deputy, which makes as much sense as anything else. OK. It makes sense, in other words.

Senator Akaka, thanks for being here.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you. Thank you very much, Mr. Chairman, for holding this hearing. I want to add my welcome to our witnesses here today.

I have long been concerned about biological attacks, especially against our food and agriculture systems. The difficulty in tracking the source of the recent E. coli outbreak in Germany and France reinforces my concerns.

A bioterror attack committed anywhere in the world could easily spread to the United States. We must detect an attack early and limit its impact, which is why we need to continue to strengthen domestic and overseas surveillance capabilities.

Dr. Majidi, last month I held a hearing on how the United States would respond to an attack on our food and agriculture systems, and an issue that was raised at the hearing was the lack of indicators of emerging threats to food and agriculture within the intelligence community.

How are the Bureau's intelligence activities targeting biological threats and, in particular, biological threats to U.S. food and agriculture?

Mr. MAJIDI. Sir, like most of the intelligence community, what we have is that annual gap review and ultimately production of what we call an intelligence requirement. That is based on what we feel has the highest risk associated with it and the information that we need to know more about that particular item.

What we do is to disseminate that particular gap through the intelligence requirement to our field offices. We share our concern with our brethren in the intelligence community, and in many instances we work collectively together to push those gaps out for additional collection.

The issue of agroterrorism and biological attacks has been on the forefront of many of our activities, and these gaps have already been disseminated, and we are still requiring additional information on many of the items.

Senator AKAKA. Dr. Lurie and Dr. Garza, as you know well, effective global disease surveillance can provide early warning to the public health community of emerging infectious diseases in other countries that could potentially threaten the United States. Would you please comment on what steps your departments have taken to make sure our Nation is aware of possible threats overseas?

Dr. GARZA. Yes, thank you for that question, Senator. In terms of biosurveillance, in particular the global reach of biosurveillance, most of the work that we have done within the Office of Health Affairs has been through our National Biosurveillance Integration Center, and in that capacity we work with many of our Federal partners, many of whom are seated here today, including the FDA, USDA, HHS, and others. DOD actually has a fairly substantial global reach in biosurveillance due to their deployment activities. And so we work with them to bring that information together into one place where we can take a look at the data to make sure that there are no signals coming out that would impart something of concern to the United States.

I think we work very well with our partners at HHS, DOD, and others to make sure that we are not missing anything and to make sure that we are covering the different aspects of biosurveillance.

Senator AKAKA. Dr. Lurie.

Dr. LURIE. I will maybe add that CDC, in particular, has a very robust global disease detection program, is one of the WHO coordinating centers for influenza, and has subject matter experts virtually all over the world helping build capacity in countries to do surveillance, working on reporting, having the relationships that give you the earlier heads up that something is coming. They also have greatly strengthened laboratory capacity in that regard.

In addition, we work through a number of organizations. The Global Health Security Initiative, which is a constellation of a number of developed countries, is actually meeting here next week. We do a lot of work and coordination with them around surveillance, preparedness, and response.

Similarly, the international health regulations promulgated by the WHO are regulations that we support, that we work through, and a lot of our efforts to strengthen detection and surveillance in countries around the world are also in support of these international health regulations.

And, finally, just because you arrived here late and did not have an opportunity to hear more discussion about this, we also have to remember that novel infectious diseases certainly know no borders and can arise anywhere in the world, and we saw with H1N1 that they arose in this hemisphere. We talked earlier about the fact that we have lost almost 50,000 jobs in local and State public health around this country, many in the surveillance area. So we have to be really careful to have our guard up and surveillance networks up in every community and all over the world.

Senator AKAKA. Thank you.

Dr. Garza, Customs and Border Protection is primarily associated with its mission to prevent terrorists, drugs, and unauthorized individuals from entering the United States. Too often the agency's important mission of protecting American agriculture from the accidental or deliberate introduction of diseases or pests is overlooked.

I have introduced legislation that would elevate the agriculture mission in CBP to match the significance of the biological threats approaching our borders.

Do you believe that enhancing agricultural inspection operations will improve our Nation's biodefenses?

Dr. GARZA. Well, I cannot speak for CBP, but I certainly feel that you are correct, that if there is an increase in the inspection capacity, that will increase our preparedness for biodefense for the Nation.

There are many aspects of biodefense that I think get overlooked somehow in their one-off effects on how they provide added deterrence or added protection, even outside of the biodefense world. The technologies and the information that we get from these different activities absolutely improve different sectors of both the U.S. Government, but also in our homeland security posture. So I absolutely think that if we improve that posture, it will pay dividends for the biothreat.

Senator AKAKA. Thank you. Mr. Chairman, may I ask another question?

Chairman LIEBERMAN. Go right ahead.

Senator AKAKA. An important potential source of information is animal health professionals. They are the first line of response to outbreaks in animal populations. These outbreaks, whether deliberate or natural, often pose a direct threat to human health.

How are your departments working with veterinarians and the animal health community to ensure early and rapid detection of disease outbreaks? Dr. O'Toole.

Dr. O'TOOLE. Senator, S&T operates the Plum Island Animal Disease Center off the coast of Long Island, and among other things, we regularly train veterinarians in the recognition and diagnosis of foreign animal diseases that hopefully they do not see in their regular practice.

In addition, Plum Island is working on developing diagnostic tests for these more exotic diseases that are not endemic to our shores, including pen-side tests that we could use to rapidly screen a lot of animals in the field.

I think your concern about agroterrorism and agriculture security is well founded. Agrodefense really is the stepchild of biosecurity. I would argue that the country is underinvesting in agricultural defense, and we need to make sure that we have a strategic plan going forward.

I will repeat, I think we should build the National BioAgro Facility in Kansas. If we do not have such a facility, we will not be economically competitive in this field, we will not maintain scientific eminence in this field, and we will not have the capacity to diagnose or respond to a foreign animal disease should one occur either through natural causes or through a deliberate attack.

Senator AKAKA. Dr. Garza.

Dr. GARZA. Yes, Senator, I think that is an excellent question. I completely agree with what Dr. O'Toole has just stated. Within my office we do have our food, agriculature, and veterinarian branch, which is led by a group of veterinarians, and they do a couple of things within Homeland Security.

First, they lead a homeland security working group which spans across the different components on all of these food, agriculture, and veterinarian issues.

In addition, we have brought Customs and Border Protection into our information cycle, our National Biosurveillance Integration System cycle, so that we can share this information on the effects on animals and plants and things like this.

CBP is currently performing risk-based inspections, and I know from reading newspaper articles in the last week about some of the challenges that they have had. I know that you have been an advocate for improving that service, and I certainly applaud that. But it is something that the Department of Homeland Security takes very seriously. We work with many of our Federal partners, with our Infrastructure Protection Directorate, and with many other people in the private sector to try and improve that sort of capability.

Senator AKAKA. Thank you. Dr. Lurie.

Dr. LURIE. Thanks. Your question is important for a whole host of reasons, including, as we have just talked about, agroterrorism, but also because so many—in fact, the preponderance of new emerging diseases in humans, as you probably know, come one way or another from animals. And so our vigilance in this area is particularly important.

I think many of our Federal agencies, certainly my office, CDC, and FDA, our Strategic Information Office, etc., all employ a number of animal health professionals both to help with the situational awareness sets of issues and to look at areas where there are synergies. Not only are there tremendous synergies in surveillance, such as some of the things Dr. O'Toole talked about, but also synergies in the countermeasure development area where many of the same techniques, platforms, and mechanisms for making countermeasures, for making vaccines, for example, in humans and animals are shared. We need to, and do, really work hard to exploit those kinds of defense synergies as well.

In addition to the surveillance areas, there is that whole countermeasure development sphere that is just so important.

Senator AKAKA. Thank you. Dr. Majidi.

Mr. MAJIDI. Thank you. Our activities are actually multifold in this area. One, the FBI really accomplishes all of its tasks through its field offices. Every year, we have a large symposium called International Symposium on Agroterrorism where we bring some of the largest manufacturers to this symposium, as well as our local field office WMD coordinators, to make sure that there is sufficient interactions between folks who work in the field as well as the major producers.

We work with USDA to make sure of their awareness of potential outbreaks as well as working with cattle ranchers and farmers across the United States as a point of interaction. Much of our work is done through our partner agencies, but we want to make sure that our involvement is clearly beneficial to both parties there.

And, last, our WMD coordinators in the field offices are really responsible for one-on-one contact with all those points of interest, and that is as part of their requirements, sir.

Senator AKAKA. Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka. Thank you very much for your questions.

Let me just ask a couple more questions because we have another panel we want to get on to. I want to get a reaction from each of you quickly to the Bipartisan WMD Terrorism Research Center report, which was generally positive about progress in this area of biodefense, but essentially said that we are not prepared to handle a large biodisaster, whether it is an attack or a naturally occurring disaster. Since I have been calling on Dr. O'Toole first all the time, Dr. Majidi, give us a quick response whether you think there is any truth to that.

Mr. MAJIDI. Well, sir, I am not necessarily sure what is the definition of a large-scale biodisaster because in my book, while five individuals were killed by the Bacillus anthracis attack, the response that was required to deal with that so-called small scale was quite tremendous from a U.S. Government perspective.

Chairman LIEBERMAN. That is true. That was the anthrax attack you are talking about.

Mr. MAJIDI. Exactly.

Chairman LIEBERMAN. Right.

Mr. MAJIDI. So the financial effects as well as the resources by every government organization was quite substantial in that case.

From that perspective, while the scale is perceived as large or small, the overall consequence management is significant in totality.

Chairman LIEBERMAN. So are we prepared?

Mr. MAJIDI. Sir, I do not think we will ever be prepared for a pandemic on an incredibly large scale.

Chairman LIEBERMAN. A pandemic or a large-scale attack.

Mr. MAJIDI. Exactly.

Chairman LIEBERMAN. Well, I think the point you are making is that though the anthrax attacks of 2001 were in a comparative sense relatively small, they caused enormous dislocation and, of course, psychological fear throughout our country.

Mr. MAJIDI. Absolutely.

Chairman LIEBERMAN. And that is quite different from the kind of metro, in terms of subways, modeling that you have done.

Dr. Lurie, what do you think of what the Bipartisan Center said?

Dr. LURIE. Well, one area in which they recognized tremendous progress actually was in the area of communications.

Chairman LIEBERMAN. Right.

Dr. LURIE. And I want to highlight that communicating with the public and bringing the public along and having them have confidence in what the government is doing to help mitigate the effects of such an attack is absolutely critical.

Chairman LIEBERMAN. How communication is during a crisis?

Dr. LURIE. Communications during a crisis I think have gotten orders of magnitude better. We have a lot of planning, pre-prepared work, and mechanisms for communication.

Chairman LIEBERMAN. That is very important. That is one of the things that this Committee, I think, has learned most about response to a WMD attack, including even a nuclear attack, that the ability to communicate with people and to tell them what to do—which may be counterintuitive. The reflex may be to get out of your

house or office and run, which may be exactly the worse thing to do. So we are much better prepared to communicate to the public in a crisis, aren't we?

Dr. LURIE. Right. Absolutely. And so the good news first.

I think their observations particularly about the major large-scale attacks are what have made us focus. One, in the medical countermeasures area on shifting to this nimble, flexible capacity to make countermeasures quickly against something we have never seen before—would that we could all work at "Contagion" speed in getting a vaccine—and to have that surge manufacturing capacity. We talked about Holly Springs being the start of that, but to be able to make countermeasures very quickly in terms of an emergency, and a huge amount of work going on that sphere. And then we have been placing a lot of emphasis on the distribution and administration of those medical countermeasures, being sure that we have a much faster capability to do that, and that we are able to support with additional personnel communities that need additional personnel support and may be overwhelmed.

I think we have made progress there. We are not all the way there, and particularly because each community is a little bit different. Again, it is those capabilities and the nimble adaptable plans that have to be put in place.

And, finally, I would be remiss again if I did not point out that our ability to respond on the countermeasure side and have the countermeasures on time is very much tied to our ability to detect early and that early warning, early detection, surveillance components that all of our departments are working on so hard.

Chairman LIEBERMAN. Dr. Garza, how about ready for a relatively small incident, not ready for a major biological attack?

Dr. GARZA. Right. I agree with everything that has been said so far, but I especially agree with Dr. Majidi where it is not going to take a large event to cause a lot of disruption in society. We saw examples of this in the past during the 2001 attacks, but also as recently as Fukushima where the country was basically depleted of potassium iodine within a week. And so if you use that as a model for what would happen at a deliberate biological attack, you can understand the sort of rush to countermeasures that would happen not just within the area that was affected, but I think nationwide. So I think that is something that we really need to consider, and that is where the communication strategy plays a large part on how we would deal with this.

Second, I am, I guess, somewhat pleased that nothing went down in the report, so at least we are not sliding back. I think we have improved a lot on different issues such as surveillance and detection. And so I am pleased with that.

One of the things, though, that has been mentioned up here a couple of times is the capacity of the health care industry to be able to withstand a large-scale attack, I think, is very troubling. I can just tell you from being an emergency room physician, I have trouble handling the emergency department every day just on a regular workload. And so if we take the Minnesota case from a couple of months ago, a person who had a case of inhalational anthrax, and the amount of resources that it took to keep that one person alive, including intensive care, multiple different physicians, and mul-

tiple different medications, and if you multiply that by the effects of a large-scale attack, the health care industry is going to be overwhelmed very quickly. Unfortunate, the paradigm for the health care industry is just-in-time care, and so there is very little surge capacity capability.

Chairman LIEBERMAN. That obviously in a difficult time in our economy, but nonetheless that is high on the list of things we need to try to do better at, that surge capacity. Dr. O'Toole.

Dr. O'TOOLE. Well, no, we are not ready for a global catastrophe involving a deadly pathogen, whatever its origin. President Obama implicitly acknowledged this last month when he called for an international effort in the surveillance and management of infectious disease, whatever the origin of the plague.

But in government, one is forced to focus on actionable priorities, and if I had a magic wand, I would wish for three things—although Dr. Garza's wish for fewer vulnerabilities and more surge capacity all across the board in terms of the response communities is a good start. We know that communication is improved, and we also know from past experience that the community's expectations of what they ought to be doing, of what might happen, are very important. There is recent research that shows just having a single person assigned to outreach with the community can make a big difference in terms of resilience and response. We ought to fund those people and make sure every State and local health department has somebody whose job is to do that. That could have a big impact. We talk about it, but we mostly wave our hands at resilience thus far.

I also think that having rapid, even point-of-care diagnostic tests that say you are infected, you are not, in an outbreak of disease, particularly at scale, is going to be critically important. The technology for this exists. There is wondrous technology that might be just within reach that would be even better. We have got to build these diagnostic tests.

And, finally, I would just offer a caution on the interagency process and the complexity of biodefense. I do believe that we have made very significant incremental progress over the past decade, but the interagency process is inherently slow and cautious. That might be the right approach when we do not know what we are doing and we do not want to make major missteps and we want to carefully husband limited resources. On the other hand, I think this is an area where the threat is growing, where the consequences are potentially so dire that the United States of America ought to make a few big bets and think about in what areas could we invest where a leap ahead would make a huge difference. Having a way to rapidly make medicines and vaccines, to surge, to do that cheaply and with fidelity, would change the world. We ought to think about that.

Creating a biosurveillance system instead of talking about it, which would start with electronic links between public health and hospitals, would make a big difference. NBAF would make a big difference. If we leave it to the interagency and biodefense is continuously peanut-buttered across all of these very hard-working agencies, we are not going to make any leap-aheads, and that worries me.

Chairman LIEBERMAN. Well, that is a good challenging note to end this on.

Do you have any more questions for this panel, Senator Akaka?

Senator AKAKA. No. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks for your service, thanks for your testimony. Just putting it all together, really we have come a long way, but as Dr. Majidi said, in this case even a relatively small biological incident can have enormous effects. And when you put that together with what we all acknowledge is all the evidence we have of the work that our enemies—and then the people who, as we found out in the anthrax case, apparently a researcher uses these pathogens for hostile purposes, this is really something to be concerned about. As we look at the list of priorities and, as you know, in a big, open, free country such as ours—and we want most especially to stay that way—it is very hard to protect against all attacks. But if you started to list the probabilities with consequences, I would say that this is an area—that is, biodefense—that really comes right to the top of certainly my priority list. So in that sense I thank you for what you are doing, and we will continue to look forward to working with you to get more and more secure. Thank you for being here.

We will call the second panel now: Dr. Thomas Inglesby, Dr. Robert Kadlec, and Dr. Jeff Levi. This means we have a total of five M.D.'s and two Ph.D.'s testifying today. Thanks to the three of you for being here and for your patience as we listened to the first panel.

Our first witness today is Dr. Thomas Inglesby, who is Chief Executive Officer and Director of the Center for Biosecurity at the University of Pittsburgh Medical Center. He was one of the center's founding members, served as its Deputy Director and Chief Operating Officer. Whatever happened to the first director?

Dr. INGLESBY. She rose in the world a bit.

Chairman LIEBERMAN. And I know you were recently named chair of the Board of Scientific Counselors to CDC's Office of Public Health Preparedness and Response. Thanks for being here, and we welcome your testimony.

TESTIMONY OF THOMAS V. INGLESBY, M.D.,[1] DIRECTOR AND CHIEF EXECUTIVE OFFICER, CENTER FOR BIOSECURITY, UNIVERSITY OF PITTSBURGH MEDICAL CENTER

Dr. INGLESBY. Mr. Chairman and Members of the Committee, thank you for the chance to speak to you today about U.S. biopreparedness 10 years after the anthrax attacks. My name is Tom Inglesby. I am the director of the Center for Biosecurity of UPMC, and as you requested, I will focus my testimony on medical countermeasure development, biosurveillance, and other issues raised in our recent center report, "Crossroads in Biosecurity."

The potential biological threats to the United States are serious. We could face a new flu pandemic that spreads like H1N1, but kills like H5N1, or a novel virus that jumps from animals to humans and spreads across the world quickly, or another biological weapon.

[1] The prepared statement of Dr. Inglesby appears in the Appendix on page 1196.

The anthrax letters of 2001, as shocking as they were, were a very small case of the use of biological weapons. Attacks in the future could affect extraordinary numbers of people.

In 2009, President Obama's National Security Council said: "The effective dissemination of a lethal biological agent within an unprotected population could place at risk the lives of hundreds of thousands of people. The unmitigated consequences of such an event could overwhelm our public health capabilities, potentially causing an untold number of deaths."

One of the most important components of our defense against biological threats is the development of medical countermeasures. DHS has issued 12 Material Threat Determinations for top biological threats to the American public. Countermeasures for just three of those—anthrax, smallpox, and botulism—have so far received the majority of funding in advanced development and procurement. Here are my suggestions for making more progress in the future on countermeasure development.

First, BARDA should convey its specific priorities, predicted budget requirements, and timelines for delivering them. Right now it is not clear, or at least it is not clear from the outside, what the top priority products are, how long it will take to develop them, or how much it will cost. And for each priority product that is to be developed, it should be made clear to what extent its development requires more basic science versus more advanced development, and the funding for this work should be allocating accordingly. If specific regulatory problems are the problem, then funding should be directed to FDA to resolve them.

When decisions are made to purchase a particular countermeasure in the National Stockpile, an explanation should be provided, to the extent possible in the public, that explains the choice and the quantity and the way it will be used in crisis.

BARDA's recent Strategic Plan places a priority on broad spectrum antimicrobials and multi-use platforms. In the long term, we absolutely do need to develop multi-use platforms and broad spectrum products. But we also need to make sure expectations are not unduly raised in the short term. There are few experts who think a shift like this is likely in the short term. So in the short term, we need very applied, very directed advanced development of products that address the greatest material threats to the country. And we should certainly stretch our biosecurity resources in the smartest possible ways, for example, by extending the shelf life of products already in the stockpile, wherever possible, and by investigating the feasibility of shortening the course of antibiotics for various diseases that we might be exposed to, and by completing dose-sparing studies that could help us vaccinate more people while decreasing costs.

In the realm of countermeasures, there are serious funding issues. There has not been enough advanced development funding as compared to basic science funding in the Federal budget for this mission, and BARDA has received a small fraction of what a private company would have required to make the same number of products. It is also our understanding that the BioShield fund will be depleted this year, and without a BioShield fund, we will not get new products procured.

And, finally, FDA was funded properly to deal with medical countermeasures for the first time this last year, but that program's budget was reduced from $170 million to $19 million in the Senate and to zero in the House. Its work would be significantly set back if the FDA got that budget allocation.

Biosurveillance is also another critical area of U.S. biopreparedness, and there have been gains but much work remains to be done. In many places biosurveillance is still too slow to discover or keep up with fast-moving epidemics. A few recommendations to improve it:

First, a small portion of the $18 billion that is now going into the electronic health record incentive program should be moved to public health in order to allow them to be able to process and analyze information related to outbreaks.

We also need to improve electronic laboratory reporting. All notifiable diseases should be automatically reported from the lab to health departments and continue to be transmitted throughout the course of an outbreak, and that does not happen now, although all in public health agree it is a top priority.

In addition, as Dr. O'Toole said, we should place higher priority on rapid diagnostics. Right now we are investing heavily in the basic science side of diagnostics, but it trails off as we get to commercialization and development, and we could change that and make a big difference.

And, finally, I want to emphasize how important public health preparedness is to U.S. biosecurity. Prior to 2001, many health departments lacked even the most basic expertise and infrastructure, and after 2001, incredible things have happened in the public health arena. New Federal funding has built a lab network, funded epidemiologists around the country, developed 24/7 response capacity, and much more. But recent declines in public health funding have directly, and very directly, threatened public health gains around the country. Federal funding for public health preparedness programs has declined by 27 percent since 2005 with a cut of more than $100 million since fiscal year 2010 alone.

If the proposed cuts take place in this year's CDC preparedness budget and preparedness efforts around the country will suffer. For example, the cuts would diminish or eliminate CDC's ability to prepare for nuclear or radiological terrorism, CDC's diagnostic program for emerging infectious diseases, their chemical laboratory and response programs, the Laboratory Response Network, and all of the academic centers for public health around the country, which is the only CDC external funding for preparedness research. I think this would be a real loss for the country, and I really would urge Congress to consider reversing the funding cuts that are planned.

So, in conclusion, the country has made real strides in preparedness over the last 10 years. I have detailed them in my written testimony—some of them, I should say—but a lot of work remains to be done. I hope the Committee and its colleagues working on the reauthorization of the PAHPA bill now in the Senate and the House will ensure we continue to make progress in the time ahead.

Thank you.

Chairman LIEBERMAN. Thanks very much, Dr. Inglesby. That was very direct, in some cases provocative, and some interesting ideas. I appreciate it.

Dr. Robert Kadlec was a career military officer physician in the U.S. Air Force—we thank you for your service—and also served in a number of senior positions at the White House, Senate, and Department of Defense, and now is a biodefense consultant to industry and government agencies. His most recent government position was Special Assistant to the President and Senior Director for Biological Defense Policy on the Homeland Security Council.

We are grateful that you are here and welcome your testimony now.

TESTIMONY OF ROBERT P. KADLEC, M.D.,[1] FORMER SPECIAL ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND SENIOR DIRECTOR FOR BIOLOGICAL DEFENSE POLICY

Dr. KADLEC. Chairman Lieberman, thank you. I am evidence of a red herring, I guess is the way to start off my comments today. I would like to thank Members of the Committee, as well as staff, and it is really a privilege to testify before you today.

One issue to put in historical context is that the efforts to prepare our country for bioterrorism predated 9/11. And, in fact, the progress that we have to date is really a testimony to three consecutive presidential administrations and several congresses in tandem. The Executive and Legislative Branches established bipartisan policies, passing vital authorizing legislation, and appropriating funds over the last dozen years. And, sir, I would note your leadership in this area. During my tenure on the Hill, working with Chuck Ludlam, your BioShield II legislation served as being, if you will, the father of the PAHPA legislation that ultimately passed.

So it really has been an achievement of bipartisanship over that period of time, and in many ways Congress has led the way to ensure improvements in State and local emergency service and public health preparedness, in research, development, and procurement of medical countermeasures, and improved hospital and first responder preparedness.

Despite the progress, I think as has already been discussed, we are far from being entirely prepared. I think the point in the question you made earlier, sir, about the difference between a small and large attack, I think, is worthy of noting the difficulty discerning the difference between wide-scale disruption and wide-scale devastation. And, quite frankly, one of the leaders that you did not have here today, Dr. Peggy Hamburg, the current Director of the FDA, really identified the dilemma back in 2005, that if the spores of one anthrax envelope had been put in the air shaft of the World Trade Center, there would have been a far larger number of casualties that died in those towers as they fell.

Chairman LIEBERMAN. That is right. I remember when she said that. That was chilling.

Dr. KADLEC. And so when you look at today's environment, and particularly the remarks of the former National Counterterrorism

[1] The prepared statement of Dr. Kadlec appears in the Appendix on page 1205.

Center Director Michael Leiter, where he expressed his concern about the risk from chemical and biological terrorism, particularly after he left his position as Director in July 2011, where he said, "The potential threat from al-Qaeda in the Arabian Peninsula is very real. The most likely . . . are simple forms of chemical or biological weapons attacks (rather than a nuclear attack)."

I am reminded daily, looking in the papers, as I look at the casualty list of young Americans who have died in either Iraq or Afghanistan, to understand that we continue to be at war with these individuals and groups who are intent on using these weapons. And I think it is worthy to note, sir, and you have already commented on the Graham and Talent report, that we have a long way to go but have covered a lot of ground in terms of some of our specific capabilities. But I am going to identify two major obstacles and one critical missing ingredient leading to improved preparedness. The beauty about them is, quite frankly, they do not cost a lot of money.

The first obstacle we have to overcome is our understanding of the difference between bioterrorism, biowarfare, and natural disease pandemics. Quite frankly, Mother Nature is not a thinking enemy intent on inflicting grievous harm to our country, killing our citizens, undermining our government, or destroying our way of life. Mother Nature does not develop highly virulent organisms that are resistant to our current stockpiles of antibiotics or disseminate them in high doses to result in more rapid onset and a more virulent clinical course of disease than seen in nature.

Mother Nature does not target our military forces to undermine our capability, or our civilian population, undermining our willingness to protect our national interest. And certainly Mother Nature does not use biological agents to achieve the lethal equivalence of nuclear weapons.

The second obstacle confronting us is embracing the greater role for the Federal Government that is inherent in our Constitution in responding to the risk particularly from deliberate biological threats. While all disasters are local, a biological attack is just that—an attack on our Nation—and our Federal Government needs to commit to a greater role in supporting and assisting State and local authorities.

And, finally, I firmly believe that the missing critical ingredient, the secret sauce, to continued progress and future success is leadership. It was the finding of the 2010 National Biodefense Science Board report to the Secretary of HHS, as well as one of the three principal recommendations of the Graham and Talent report card. Without strong leadership that emanates from the White House, that is propagated through the Federal departments to State and local authorities, no amount of money will make us sufficiently prepared. We saw some of the leaders that sat on the first panel here today.

The White House has already demonstrated such leadership with its commitment against the threat from nuclear proliferation and cyber attacks, but biological weapons can kill more than cyber attacks and are easier to develop, as you noted, sir, than nuclear weapons. Without the President's visible concern and commitment, the best efforts of many capable people of his Administration will

be wanting. White House involvement is essential to ensure that departments and agencies live up to their interagency obligations under the National Response Framework and emergency support functions.

Just to highlight two in particular, the role of the Department of Defense and the role of the Department of Veterans Affairs in the response to surge capacity, for example, the involvement and contribution of those two agencies have not been entirely optimized.

Visible leadership is not only a requisite for the Executive Branch, but as you know, sir, Congress has a vital leadership role as well. Congress can and has effectively advanced preparedness through legislative initiatives, oversight, and appropriations, and I understand, sir, your Committee is considering legislation to complement the bill created by your colleagues in the House. And I also understand there are efforts in the Health, Education, Labor, and Pensions Committee to reauthorize the Pandemic All-Hazards Act to complement the bill passed out of the House Energy and Commerce Committee. Hopefully, Congress will act to pass one or, ideally, both bills before the end of this session.

Finally, I offer one last observation and thought. The grades issued by Senators Graham and Talent are useful to assess where we stand, but they are, frankly, abstract to the grim reality they represent. As a military physician who served in two conflicts, Desert Storm and Iraqi Freedom, I know too well that in war, grades do not matter. Combat is a pass-fail test. Simply stated, accepting getting a D or F grade means many Americans may die needlessly in the event of an attack. This is not only unacceptable, but as public servants, we would be derelict in our duty if we did not do everything in our power to prepare our country and protect our citizens from this risk.

I look forward to your questions. Thank you.

Chairman LIEBERMAN. Thank you, Dr. Kadlec. That was excellent and also raised some good questions, which we will come back to.

Dr. Jeffrey Levi is Executive Director of the Trust for America's Health.

In January of this year, President Obama appointed Dr. Levi to the Advisory Group on Prevention, Health Promotion, and Integrative and Public Health. In April, he was appointed chair of that group. He is also a professor of health policy at the George Washington University's School of Public Health, where his research is focused on HIV/AIDS, Medicaid, and integrating public health with the health care delivery system.

That is an impressive resume, and thanks for being here today.

TESTIMONY OF JEFFREY LEVI, PH.D.,[1] EXECUTIVE DIRECTOR, TRUST FOR AMERICA'S HEALTH

Mr. LEVI. Thank you, Mr. Chairman, and I am grateful for the opportunity to testify before the Committee on the progress and challenges we face on the 10th anniversary of the terrorist attacks on our Nation.

[1] The prepared statement of Mr. Levi appears in the Appendix on page 1213.

I am going to focus on public health's role, which is crucial, in emergency preparedness and response. Health departments perform the surveillance that detects the first cases in an outbreak. Laboratories test the samples. Epidemiologists conduct the investigation and pinpoint the source. And public health workers coordinate the medical response, advise and communicate to the public, and distribute vaccines or drugs that help save lives.

The anthrax attacks were a great wakeup call to the need for greater investment in public health preparedness, and over the last decade we have made dramatic progress in meeting this responsibility. But, unfortunately, it seems that we have hit the snooze button because that progress is greatly threatened by recent funding cutbacks at the Federal, State, and local level, and we could face the sad irony that if another attack were to occur today, we may be better prepared than we were 10 years ago, but possibly not as well prepared as 3 years ago.

Last month, Trust for America's Health and the Robert Wood Johnson Foundation released a new report, "Remembering 9/11 and Anthrax: Public Health's Vital Role in National Defense." In developing this report, we learned that the public health system mounted an extraordinary response to these events despite limited familiarity with bioterrorism and decades of underfunding that left it with a deficit in technology, workforce, and training.

For example, in 2001, there was not a clear public health response system in place for handling unexpected emergencies; thus, much of the response was developed on the fly.

There was little to no experience in countermeasures research and development, and CDC and health departments faced a crushing demand for information and recommendations that had not been prepared in advance.

Despite these challenges, public health rose to the occasion. The Laboratory Response Network, which is now an integral piece of the BioWatch program, tested 350,000 environmental samples and clinical specimens over an extended period. CDC provided national surveillance, laboratory diagnostic support, treatment recommendations, and advice on post-exposure prophylaxis. And public health helped to calm a Nation by putting science first in risk communications.

Since fiscal year 2003, Congress has invested over $12 billion in State and local public health preparedness, hospital preparedness, and State and local pandemic capacity. This outlay has led to tremendous progress in our ability to prepare for and respond to an emergency. Now we recognize that bioterrorism and emergency preparedness are integral to the role of public health and that public health is integral to disaster preparedness and response. We have fully developed rapid response capabilities so that health impacts are considered and mitigated from day one of an emergency.

Unfortunately, these improvements cannot be maintained with one-time investments. Training of our public health workforce must be ongoing; vaccines and antivirals in the Strategic National Stockpile are expiring; technology is quickly becoming outdated; and health departments need predictable funding to operate laboratories, respond to emergencies, and investigate outbreaks. And yet Federal support for public health preparedness has been cut by 37

percent since fiscal year 2005. Moreover, the cuts at the Federal level have been matched or exceeded at the State and local level. As a result, I worry deeply, as do my colleagues on the front line of public health agencies, that our capacity to respond to a new emergency will be severely diminished in the near future.

These budget cuts are not just about money to purchase supplies and equipment. They are about the people who are essential to an effective public health response. Were a major public health emergency to occur today, even compared to the demands of the pandemic H1N1 just 2 years ago, there might not be enough workers to effectively respond. Forty-four thousand State and local public health positions were lost since 2008. We simply cannot quickly hire and train a 21st Century public health emergency workforce after an attack occurs.

There is one silver lining here. Since the creation of the Prevention and Public Health Fund, we have put over $60 million in epidemiologial and lab capacity across the country at the State and local level, but that funding is also at risk, and if we lose that money as well, we will be in even worse shape.

We also need to fundamentally rethink how we do surveillance for both emergencies and routine public health issues. Our disease surveillance system has been built one disease or crisis at a time, resulting in archaic and static silos of information. The particular challenge in the field of preparedness is that we do not necessarily know in advance what we will need to know. And, thus, the most comprehensive approach to data collection is needed.

We must also harness the opportunities afforded by the Nation's transition to health IT systems with electronic health records at their core, and I think you heard from previous witnesses the degree to which public health needs to be at the table in the design and development and implementation of these processes, or else they will not help us in the area of preparedness.

Our report found that the United States often takes a band-aid approach to public health preparedness. As new emergencies and concerns emerge and attention shifts, resources are diverted from one pressing priority to another, leaving other ongoing areas unaddressed. I am encouraged to see this Committee is taking these threats seriously, and I thank you again for the opportunity to be here today and look forward to your questions.

Chairman LIEBERMAN. Thanks, Dr. Levi, very much. I was really struck by one line from your testimony, which is the effect of funding cuts: ". . . the sad irony is that if another anthrax attack were to occur today, we may be better prepared than 10 years ago—but possibly not as well as 3 years ago." And this is part of the effect of the budget deficit crisis we have gotten ourselves into. We have to be very mindful of it.

I want to ask you at the beginning what you think of, to me, an interesting idea that Dr. Kadlec mentioned, which is, at least in part, to try to ameliorate this problem with regard the need for a public health surge in response to a biodisaster or a bioattack by being prepared to utilize personnel from the Department of Defense and/or the VA.

Mr. LEVI. I think Dr. Kadlec was referring to health care personnel, and that is certainly——

Chairman LIEBERMAN. Correct. That was my assumption.

Mr. LEVI. Right, and that certainly is appropriate, and I think there are plans on the table, and how well they have been exercised is another question. But I think all of those agencies are committed to doing that kind of collaborative work.

That is once we have identified what is going on, but my concern with personnel is that the day-to-day public health capacities of detecting, identifying a pathogen, communicating with the public, disseminating countermeasures, those kinds of things that are a core public health function. We have lost 44,000 workers. We have lost people who are trained. It requires special expertise, and it requires expertise that is exercised over and over again so we keep improving. That capacity is dramatically diminished compared to 3 or 4 years ago, and if the budget cuts that seem to be on the table now go forward, it will even be worse.

Chairman LIEBERMAN. I wish I could be encouraging about that. In the short run, it is very hard to be. Hopefully we will get the economy going again. But, of course, particularly in the stress that we are under now in terms of our budget, this should force us to make priority judgments, and by any number of standards this is a priority for us. To me it is part of the constitutional responsibility to provide for the common defense, really.

Dr. Inglesby, you pointed out something that I think there is not enough awareness of. It is a fact that over the last 10 years, the Federal Government has made significant progress, building on progress before, and developing medical countermeasures such as vaccines and therapeutics to anthrax, smallpox, and botulinum. But as you point out, those are just 3 of the 12 agents that the Department of Homeland Security identifies as representing a material threat to our country, and that does not even include the emerging threats of someone manipulating substances, for instance, in a laboratory.

Dr. INGLESBY. Right.

Chairman LIEBERMAN. So I wanted to ask you, first off, if you accept the rationale behind the listing of these 12 and whether you think the prioritization of the medical countermeasures, that is, on behalf of the Federal Government, is clear enough.

Dr. INGLESBY. I do think the material threat determination process is very rigorous. As an outsider, I have seen a couple of the processes play through, and I have been very impressed with the rigor and the science. The details of the specific ordering right now I think is not public, so I cannot comment on that.

Chairman LIEBERMAN. Right.

Dr. INGLESBY. But, in general, I think that it is a very rigorous process, and it is like what is done in other parts of the government. You set requirements and then the government reacts accordingly, and you set requirements as scientifically and rigorously as possible.

So I think it is the right place to start with, actual requirements that there is wide agreement on in the government, and then to work backwards from that.

Chairman LIEBERMAN. Good. In the medical countermeasure review that Health and Human Services released last year, they pointed out a number of things that they are going to do to improve

the development of medical countermeasures such as including particularly the one that Dr. Lurie talked about, creating government manufacturing centers, partnering with the private sector and strategic investment firms, as well as moving to products that address multiple threats and, finally, to streamline FDA regulation.

Give us your reaction to those recommendations, and how would you prioritize those? Which do you think offer us the most hope of making more rapid progress?

Dr. INGLESBY. Well, starting with the last first, I think there is total agreement in and out of the government that FDA needed more resources and a lot more heft behind its program, and it has gotten it in the past year. So I think that was a really important development.

I think there was also a part of that review that said there should be more integration between the various parts of government, NIH, BARDA, FDA, and CDC. I think that is very important.

Chairman LIEBERMAN. Right.

Dr. INGLESBY. When we have a requirement on the table, have we sorted out exactly what is required in the realm of basic science? Does that relate to advanced development? Does it relate to what is going to go in the stockpile, its regulatory problems? I think that is a very important facet of the strategy.

As regards the Centers for Innovation and Advanced Development, I certainly believe in the principles behind that program, and we were supportive of that for a number of years as it was being discussed. In principle, it is a way to engage large pharmaceutical companies, which would be great for the country. It is actually probably crucial in the years ahead to get the talent of large pharmaceutial companies. And, in principle, it was a way to consolidate the costs and reduce the costs and concentrate expertise. And, in principle, I think it was a way to foster innovation.

I do not know how it will play out. I have to say, in terms of making my conflicts available to your Committee, our mother institution was a potential competitor for that program and has decided not to compete.

Chairman LIEBERMAN. Right.

Dr. INGLESBY. But I hope that it succeeds. I certainly favor its original principles, and we will have to see how it ends.

Chairman LIEBERMAN. Dr. Kadlec, let me bring you into this because you mentioned Chuck Ludlam who used to work with me. He is really creative, and he had an idea which I thought was a great idea. What do we do to get the big pharmaceutical companies into this field? Because it is not a naturally attractive market. So, Mr. Ludlam had the idea—and I put it forward; I think Senator Orrin Hatch was with me on that one—to say to big pharmaceutical companies, if you develop a medical countermeasure that HHS determines has some promise or passes a threshold, then go ahead with it, and we will give you the right to choose one of the array of drugs you have and extend the patent for 2 years.

Well, it was as if we had sounded the trumpet for battle, and the generic drug manufacturers came marching with great force over the Hill and killed that idea.

I am not saying it is the only idea out there, but it was, I think, a creative attempt to deal with this problem. I wonder with the passage of years whether you have any other thoughts about how to make sure that we develop medical countermeasures, beginning with those nine other agents that the Department has said we have to worry about.

Dr. KADLEC. Well, sir, I certainly was around during the time of the wild card and certainly do remember. I think I have a few trample marks on me from the generics. [Laughter.]

But the issue is really about the role of big pharmaceutical companies here, and their interest and appetite to be involved seems to involve two areas. One is the issue of risk and, quite frankly, the other one is the issue of profit. Obviously, the "wild card" option certainly was an incentive on the profit side, and there has been much, I think, to address the risk side subject such as the Public Readiness and Emergency Preparedness Act, which had to do with liability. So in some ways, that barrier has been lowered.

The other part of risk is technological risk and, if you will, where I think the government is trying, and appropriately so, to establish that there are opportunities for big and small pharmaceutical companies to get involved in places where co-development of new technologies. Platform technologies that could be used for biodefense that have direct commercial relevance and applicability and the assurance that the FDA would consider these as not only commercial but also national security-viable technology approaches is certainly another incentive. The question is whether that is enough, and, quite frankly, I think we still face the challenges with big pharmaceutical companies where they still view the profit incentives to be somewhat limited.

I do not know if we will ever get over that hurdle, but I do believe that in some ways engaging them in terms of opportunities where they can expand their technology set, where they can defer the risk of development particularly of platform technologies goes a long way. And there may be other sweeteners involved subject to some of the orphan drug status that could be given particularly to biodefense countermeasures. But it is a very difficult balance to entice them to the table.

Now, the "wild card" option here in another sense is the evolution or natural evolution of the big pharmaceutical company blockbusters where they seem to be kind of going away, where they are looking for smaller products.

Chairman LIEBERMAN. That is true.

Dr. KADLEC. And so in some ways there may be a new landscape to engage them.

Chairman LIEBERMAN. Interesting. Yes, good idea.

Dr. KADLEC. So I would say do not give up the "wild card" option just yet.

Chairman LIEBERMAN. But the reality is that if we were attacked by one of those nine other biological agents, we do not really have medical countermeasures for those now, do we?

Dr. KADLEC. That is correct. I think the answer is that the pipeline has been focused deliberately on some of the highest threats—anthrax, smallpox.

Chairman LIEBERMAN. Yes, sure. Right.

Dr. KADLEC. But, yes, the sequencing of other things that are less notable—tularemia, for example, and other threats on that list—have not probably been given the appropriate recognition or resources.

Chairman LIEBERMAN. Did you want to add something, Dr. Inglesby.

Dr. INGLESBY. I was just going to agree with what you just said, yes.

Chairman LIEBERMAN. That ought to get our attention, and some of those—am I right?—are not that complicated to make, to bring together.

Dr. INGLESBY. Well, I think any drug or vaccine is complicated——

Chairman LIEBERMAN. No, I mean the threat.

Dr. INGLESBY. Sorry, the threat.

Chairman LIEBERMAN. Yes.

Dr. INGLESBY. Yes, I mean, the things on the list—all of those agents are available in the world to acquire.

Chairman LIEBERMAN. Right.

Dr. INGLESBY. And many of them are causing outbreaks in the world in any given month.

Chairman LIEBERMAN. Dr. Garza was kind enough to stay, so there is always a danger inherent in that, but I am going to quote something from your testimony—Dr. O'Toole is here, too—and ask the witnesses for a response.

Dr. Garza indicated in his testimony that, following some kinds of biological attacks, ideally we would need to detect and start mass dispensing treatments in as little as 1 to 2 days. And I wanted to ask you—and I really should have asked Dr. Garza, too—whether, to the best of your knowledge, there is any city, for instance, that is able to meet this expectation for a wide-area attack for even just one of the biological threats we face. Dr. Levi, do you know?

Mr. LEVI. I cannot answer that question with specificity, but I think it speaks to the incredible importance of not losing more of our public health workforce, because you cannot create this kind of pop-up capacity.

Chairman LIEBERMAN. Right. Good. Anybody else?

Dr. KADLEC. Sir, I would just comment I think that there is still a lot of doubt and concern about it. I know during my tenure in the White House in late 2008 we had serious concerns. Just to note that President Obama signed an Executive Order in December 2009 mobilizing Federal assets to help assist in the dispensing effort, particularly the role of the U.S. Postal Service, the Department of Defense, as well as trying to use other Federal employees and other agencies to also assist.

Quite frankly, there are two challenges here. One is, if you will, the tyranny of time that is created by, one, the natural epidemiologies of diseases and the potential effect of high dose exposures that basically change the normal incubation period, resulting in some of these diseases to appear much faster.

The second issue is what will be the public demand and outcry. You can vividly imagine the CNN moment when this becomes first realized, an attack has happened, either through a BioWatch detec-

tion or the first case. There will be an incredible demand on the system for these antibiotics and other protective measures.

So the sooner the better, and, quite frankly, it is clear that we are probably not fast enough yet.

Chairman LIEBERMAN. Dr. Garza, we allow audience participation here. Do you want to respond to the question, which is: Is there any city or metropolitan area able to meet that standard that you raised?

Dr. GARZA. I think, Senator, that is an excellent question. There has been tremendous work that has been done in the past couple of years, both with the CDC as well as the Federal interagency, in trying to develop that capacity. Dr. Kadlec is entirely correct on those challenges to getting the medical countermeasures out to the population. But we view it as multidisciplined approach, so you have, for instance, the postal model; we are trying to engage more to get the private sector involved. As part of the Executive Order, the President directed his Administration to develop ways of dispensing countermeasures to mission-essential people. So it is a multi-dimensional approach to this problem.

Chairman LIEBERMAN. While I have you there, because we are focused on the Postal Service, unfortunately, in other ways, take a minute and tell us where we are in the exploration of using this remarkable national network of the Postal Service to help in terms of biodefense.

Dr. GARZA. Yes, sir. To my knowledge—and HHS ASPR runs most of the programs to do this—the program that has been developed and is the most widely known is the one in Minneapolis. If I believe correctly, I believe there are three or four other cities that are exploring the options or have developed plans to use the postal option. But, again, I would emphasize that it is one part of a multilayered approach, albeit an important one, but it has to be thought of as a multilayered approach.

Chairman LIEBERMAN. And there, just to be specific, we are looking at the postal men and women delivering vaccines, for instance, or distributing vaccines.

Dr. GARZA. They would be distributing medical countermeasures, so antibiotics.

Chairman LIEBERMAN. I am sorry. Antibiotics, right.

Dr. GARZA. Yes, sir. So they would be delivering antibiotics to the population's homes.

Chairman LIEBERMAN. I think that is important to continue to explore.

Dr. KADLEC. Just to put a finer point on that, because there are three cities that are in line to basically follow Minneapolis: San Diego, Boston, and Philadelphia. Those cities have received grants from HHS through the Cities Readiness Initiative to do so. So it is, again, as Dr. Garza has said, part of a multipronged approach, but the postal option really represents a first strike capability, which can in 12 hours to basically delover a limited supply of antibiotics to every residence within designated zip codes.

Chairman LIEBERMAN. So obviously the Postal Service is in real financial trouble, but part of what we are trying to do—it happened to come under the jurisdiction of this Committee—with the Postmaster General is to look at ways we can capitalize on the unique

national network they have. As you probably know, for instance, FedEx and UPS use the U.S. Postal Service for the last mile of delivery in a lot of cases where it does not make financial sense for those very successful companies to do so. And in the same way, this is an existing network which, as you say, can deliver antibiotics in a crisis very quickly.

Dr. Inglesby, you made a really interesting suggestion, and I want to ask you to develop it a bit. It begins with the fact that in the so-called stimulus act, the American Recovery and Reinvestment Act of 2009, there was appropriated $18 billion for the improvement and modernization of health recordkeeping, a general description. So you are suggesting today—and, again, I presume this is all about priorities—that some part of that ought to be reallocated to this particular problem. So talk in a little more detail about what you have in mind.

Dr. INGLESBY. So right now, if there is an outbreak in Washington, DC, the health department, who is going to be asked to figure out what is going on, has to actually walk over or phone somebody to try and go through the medical records one by one on paper. And this new program holds out the hope that you could connect health departments and clinical outpatient offices or inpatient in the hospital in an electronic way where people from their desks in the health department could try and actually go in and understand what is happening in a hospital or in a clinic automatically and analyze it and try and figure out if there are patterns going on in the hospital of this new outbreak.

The $18 billion is set up to provide incentives to the hospitals and to the doctors to develop electronic health records, and there is a series of criteria that are laid out in order to get that money. If we changed, even modified a few of those criteria a little bit to say they have to be able to be read by public health departments in a crisis, then we could use a little bit of that money to help solve a very big divide between public health and clinical medicine.

We had a meeting about this recently in our center, and the public health officials who see all this happening are upset about it because there has not been a dollar provided. They see that these electronic health records are being created, but public health is basically on the sidelines. They do not have any money to build their own IT systems to receive it. They do not have any incentive to connect nor any database management capacity. So a little bit of money could go a long way.

Chairman LIEBERMAN. Excellent idea.

Mr. LEVI. If I could add to that, Mr. Chairman?

Chairman LIEBERMAN. Yes, go ahead.

Mr. LEVI. I think it is important to think about the money that is being invested for electronic health records in the context of health reform—it is certainly a critical piece—and that the system we are designing is responsive to public health needs as well. But I think I would also add that we do have a receipt question as well, which is whether existing infrastructure in a lot of health departments even with those requirements would be able to receive and properly analyze the date. And I think that is a standard-setting and a training issue for public health agencies.

And I think I would add that we spend, just in the core work of CDC and the money they send out to the States, a lot of money on public health surveillance. That whole system needs to be redesigned, and with the redesign of that system, we may actually find the capacity and the resources to do a lot of the things that are needed on the preparedness side as well.

Chairman LIEBERMAN. Those are very constructive suggestions, and we will see if the Committee cannot move them into the system.

Dr. Kadlec, a final question. In your testimony you put a lot of emphasis on leadership, and, of course, I agree with you. It is always a critical component, sometimes overlooked because we get focused on details of what you want to do and forget the leadership. So is there a criticism there? Do you think we lack effective leadership in this biodefense area right now?

Dr. KADLEC. Well, I would just put it in—use a football analogy—we have a lot of great assistant coaches. You saw many of them. Some are still here.

Chairman LIEBERMAN. Right.

Dr. KADLEC. Where is the head coach? And where is the head coach basically making this a cause celebre—not to make a rhetorical statement around this, but as I did in my tenure at the White House. Someone needs to be the advocate and educate around this issue, particularly at the political level where there is little familiarity with it. I think there are many in the current White House who are experts on the nuclear issues. Certainly the pressing issues around cyber warfare and cyber attacks on our country and our economy have driven it in a different way.

The risk of bioterrorism and biowarfare is one area that, quite frankly, needs similar kinds of leadership. I think Dr. O'Toole identified some of the leaders there now. That is very important. But, literally, you have to have someone 24/7 whose only job is this. I am convinced, having lived it and breathed it for a period of time, where you can basically go into those meetings and fight toe to toe with OMB to ensure that they do not necessarily decrement your program because they just do not understand the national security component to it.

A quick example. In the recent budget alignments where OMB went through the exercise to basically significantly decrement a variety of different accounts, clearly homeland security and national security were treated differently. But health programs were not, and, quite frankly, the biodefense program, particularly within OMB, is buried in the Centers for Medicare and Medicaid Services. And so in some ways it takes a greater haircut than maybe some of the other programs would because just simply the recognition is not there that this small amount of money, even though it is not, about $7 billion, is like any other billion dollars that are devoted to health and other related programs. And I think that is the challenge that you have, and unless you have someone at that level to advocate and to educate—and, literally, I had to bring people sometimes kicking and screaming to the White House and interagency meetings, to ensure that they understood the equities for the country and national security.

Chairman LIEBERMAN. So you are talking about not somebody, for instance, in the Department of Homeland Security but somebody in the White House, presumably in the National Security Council, who would be designated as the person in charge of biodefense.

Dr. KADLEC. I think that is necessary but not sufficient, to get to Dr. O'Toole's point. I mean, I think the fact that if you have the right constellation of leaders across the interagency, that is also critical. But it also helps to have someone at the White House level where particularly for some of these intractable problems, subject to the integration of our biodefense medical countermeasure portfolio, or the issue of basically leveraging Department of Defense or VA to make their medical capabilities available in case of surge, or security for medical countermeasure distribution by the Postal Service, those are things that sometimes are best done at a level above that. But you need all of it. You just cannot have some of it.

Chairman LIEBERMAN. I think we have taken enough of your time, and I am going to go on to another meeting. This has been a very constructive hearing. The first panel was excellent. You built on the first panel with some very good suggestions that I think will guide the Committee as to where we can try to be supportive here. I appreciate your testimony and all the work that you do in this area very much.

We are going to keep the record of the hearing open for 15 days for any additional questions or statements for the record.

With that, I thank you again, and the hearing is adjourned.

[Whereupon, at 12:29 p.m., the Committee was adjourned.]

TEN YEARS AFTER 9/11: THE NEXT WAVE IN AVIATION SECURITY

WEDNESDAY, NOVEMBER 2, 2011

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:33 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, presiding.

Present: Senators Lieberman, Akaka, Carper, Pryor, Landrieu, Collins, Paul, and Moran.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS [presiding]. Good morning. The hearing will come to order.

Senator Lieberman, the Committee's Chairman, has been unavoidably delayed. He will be joining us shortly, but he has asked me to proceed to convene the hearing and delivery my opening statement. In fact, he suggested that I give a very lengthy opening statement in order to allow him to proceed with his before we call on our first witness. [Laughter.]

Nevertheless, we will proceed as normal.

By targeting our airplanes, al-Qaeda succeeded in killing nearly 3,000 people a decade ago. Aviation security is clearly critical to homeland security. We Americans have demonstrated our willingness to endure enhanced security measures at our airports if those measures appear to be reasonable and related to real risks. But travelers become frustrated when security measures inconvenience them, apparently without cause, or when they appear to be focused on those who pose little or no threat.

Next month, it will be 10 years since the shoe bomber failed to take down his flight from Paris bound for Miami, yet we still take our shoes off. In 2006, British and American intelligence thwarted an effort to conceal explosives in liquid bottles. We still cannot carry on a regular-sized tube of toothpaste onto an airplane. The Christmas Day bomber hid explosives in his underwear and media reports indicate that terrorists have shown interest in having explosive devices surgically implanted in their bodies. These threats have led to more intrusive pat-down searches, and one wonders what more will be required of airline passengers in the future.

We see TSA putting the very young and the very old through intrusive and, in most cases, unnecessary screenings. At the same time, it troubles many Americans to learn that a young man was

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00339 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

able to fly cross-country without a valid government ID and with an expired boarding pass that was not even issued in his name. If we continue to give extra screening to individuals who appear to pose no threat, yet others who should arouse suspicion can get past checkpoints without being questioned, our systems still are not as finely calibrated as they need to be.

Since our June hearing, the Administration has implemented a risk analysis to improve the screening process, a welcome change. This effort should provide a more effective and efficient use of the government's limited screening resources. I am encouraged, for example, that this new risk-based approach is designed to permit TSA to learn more about travelers through information they choose to provide. Some of the changes will also respond to several of our most common airport screening complaints. Secretary Janet Napolitano said in September that frequent flyers who opt in to a known traveler program will often be able to keep their shoes on and their laptops in their bags. TSA, to its credit, and Administrator John Pistole deserves credit for this, also has changed the screening procedures for children under 12, a common sense decision that was overdue.

Nonetheless, questions remain regarding how some security procedures affect Americans' privacy, their health, and whether or not the procedures are as effective as they should be. In August, TSA began installing new software in passenger screening machines designed to enhance traveler privacy. Using a generic outline of passengers, Automated Target Recognition, detects items that could pose a potential threat. I first saw this less-invasive technology in Amsterdam in 2010 and I repeatedly raised this issue with Administrator Pistole and Secretary Napolitano. This technology was implemented at Schiphol Airport in the wake of the Christmas Day bomber who was able to go through that airport with his explosives undetected.

I would parenthetically note that I assumed that this was some cutting-edge technology that had been developed in Germany. I asked where it had been developed and was told in Massachusetts. So, clearly, there are opportunities within our own country to take advantage of new technology.

I urged consideration of this software, which better respects travelers' privacy, eliminates the need for a separate screener in a booth, relies less on human judgment, and eliminates the inconsistencies associated with human reviewers. I am very pleased that TSA is rolling out and testing this technology.

While the ATR technology is currently being used with so-called Millimeter Wave Machines which use radio frequency energy to generate images, I would note that other Advanced Imaging Technology, screening machines use backscatter X-ray radiation that have continued to raise health concerns. This is an issue that I hear about from my colleagues all the time because most of us travel every single week. I also hear about it from pregnant passengers who are concerned about the exposure to the babies that they are carrying. DHS, in my view, should independently evaluate the health effects of that technology and establish a goal of using radiation-free screening technology.

Let me underscore my appreciation of the fact that no single screening technology can ensure our safety. There is no magic bullet. There is no perfect system. And that is why a layered system of security is so essential, involving watch lists, intelligence, and all the tools at our disposal.

The fact is that we face a determined, innovative foe, and no machines can substitute for good intelligence, well-trained screeners, and an observant public. The passenger screening process has received both attention and sometimes anger from the traveling public. It became clear last year, however, from the printer cartridge plot, that cargo security is also a threat that terrorists are investigating. That is why Senator Lieberman and I intend to introduce an air cargo screening security bill later this year. Our successes in risk-based screening of maritime cargo should provide a road map for risk-based screening of air cargo, and that is what our legislation is intended to do.

And, of course, just in the past 24 hours, we have learned of gaps in our security related to certain catering operations at Atlanta's main airport. Those are very serious concerns because, obviously, the catering personnel have direct access to materials that are put on airplanes, and I am sure that is an issue that we will be talking about this morning.

Our government's first priority is to protect against terrorism and the public will accept a certain level of intrusion and inconvenience at our airports, as long as we are convinced that it is enhancing our safety. But DHS should continue to expand the use of risk-based approaches to screening with technology and techniques that are safer, more effective, and that minimize privacy and health concerns.

Now, at this point, I would usually say, "Thank you, Mr. Chairman," but in this case I would be thanking myself.

We are going to move to our first witness today. We are very pleased to have with us John Pistole. He is the Administrator of the Transportation Security Administration within the Department of Homeland Security.

Mr. Pistole, we welcome you back to the Committee. I, for one, want to commend you for your hard work and for being very open to our suggestions and to the recommendations of the public as you seek to protect the traveling public. Please proceed with your testimony.

TESTIMONY OF HON. JOHN S. PISTOLE,[1] ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PISTOLE. Well, thank you, Senator Collins, and thank you for the Committee for your support of our Risk-Based Security Initiative in terms of how we try to work to provide the most effective security in the most efficient way.

So when I last appeared before this Committee, as you noted, our plans to deploy aspects of this Risk-Based Security Initiative were still being formulated. I am pleased to report that we have begun actually implementing several aspects of risk-based security in

[1] The prepared statement of Mr. Pistole appears in the Appendix on page 1230.

some airports and testing other aspects in other airports around the country, again, with the goal of providing the most effective security in the most efficient way.

As this initiative progresses, we must ensure that each step strengthens security as intelligence informs us of terrorists' ongoing interests in attacking aviation, and as noted, because most air travelers present little risk of committing an act of terrorism, the goal is to focus on those who present the greatest risk. Anecdotally, we still find four to five guns at airport security checkpoints every day. Yesterday, we found six, including one at Chairman Lieberman's Bradley Airport in Hartford, Connecticut, a loaded gun with seven rounds in it in a checked bag that was going to try to get through.

Our success in discovering other non-metallic items is significantly enhanced through the use of Advanced Imaging Technology, as you noted, because these machines give us the best opportunity to find non-metallic threats such as we saw on Christmas Day 2009 and have successfully detected items as small as a coin or even a small individual piece of gum that is wrapped. AIT, of course, is not perfect, as you know, and we continue working closely with manufacturers to improve its detection capability, but again noting that it does give us the best available opportunity from a technology perspective of detecting those Christmas Day-type bombs.

Additionally, as part of Risk-Based Security Initiative, we recently deployed TSA Pre-Check, a voluntary passenger pre-screening initiative with a small known traveler population in four U.S. airports, placing more focus on pre-screening individuals who volunteer information about themselves prior to flying. Because we know more about them, TSA Pre-Check travelers may move more swiftly through the standard screening process and be able to divest fewer items, such as leaving their shoes, belt, and a light jacket on along with keeping their laptop in their briefcase and keep their liquids, aerosols, and gels in their carry-on bag. Of course, we will always incorporate random and unpredictable security measures throughout the airport. At no point is a traveler guaranteed expedited screening.

Initial feedback for TSA Pre-Check has been very favorable, with approximately 40,000 travelers having gone through this expedited screening process so far. Our first two partner airlines, American and Delta, have successfully demonstrated the required technical capabilities and we are working with other airlines and other airports to expand the program as they become operationally ready and as more and more people sign up through Customs and Border Protection's hugely successful Global Entry Program.

Efforts to expand identity-based screening are also evident in a new crew member screening system which helps positively verify the identity and employment status of airline pilots. Under this program being tested at seven airports currently, tens of thousands of airline pilots have processed through this expedited screening, again, all with very positive feedback.

We are also evaluating an expanded Behavior Detection Initiative that began this fall at Boston Logan Airport and now Detroit Metropolitan Wayne County Airport. In this new initiative, behavioral analysis techniques are used by specially trained officers to

determine if a traveler should be referred for additional screening. This additional interaction used by security agencies worldwide enables officers to better confirm or dispel suspicious behavior and anomalies. Preliminary analysis from Boston shows an increase in detecting high-risk passengers, but additional data is required, both to understand if that trend is statistically significant and to measure it against our return on investment.

In August, we implemented, as you noted, a new screening procedure for children 12 and under, allowing them to leave their shoes on and go through a less intrusive security screening, recognizing that intelligence indicates that these travelers pose little risk to aviation security, although, of course, it can be used by those who might want to cause harm. These changes give our officers more options to resolve any alarms that may occur during the screening process. The results from this nationwide enhancement to screening show a sharp reduction, although not elimination, of the need for a physical pat-down for children and families have responded very favorably to these changes.

Combined with TSA Pre-Check and known crew member screening, these new processes help us free up resources to focus on higher-risk travelers. In essence, risk-based security helps us strengthen security by reducing the size of the haystack in which a terrorist might be hiding. I am dedicated to further identifying additional groups as part of the High-Risk Security Initiative and I look forward to updating this Committee as these efforts progress.

So in closing, innovation, partnerships, and a commitment to the pursuit of excellence, these are the watchwords of TSA as we move into 2012.

Thank you, Senator Collins and Members of the Committee, for the opportunity to appear before you today. I look forward to answering your questions. Thank you.

Senator COLLINS. Thank you very much, Mr. Pistole.

As we have seen over the years, terrorists continue to look for gaps in our aviation security procedures and that is why I was particularly disturbed to read of a local TV report in Atlanta, Georgia, where lax airline catering security procedures were identified through an investigative report and an undercover video. And specifically, press reports indicate that the video showed catering employees piggybacking through security checkpoints. There were unsealed catering carts, which obviously would allow explosives or weapons to be concealed among the food in those carts, that were in the staging area before they were being loaded onto the plane.

What is TSA doing in response to this report? Have we identified yet another vulnerability, or do you believe this is an isolated incident?

Mr. PISTOLE. Thank you, Senator, and clearly, this is something that we take seriously and is a concern under the umbrella of the insider threats. So those who have some type of special access, either through their work, employment, and their backgrounds, allow them access in a way that the general public does not have is something that we focus on. We set standards for catering companies and airports around the country, that they have to meet these standards. We inspect to those standards. So when we get a report

such as this, that there has been some type of breach or vulnerability identified, we move very quickly.

So in this instance—this was brought to our attention in the last month—we immediately sent a team to Atlanta to work with the airport but also the catering company to assess what vulnerabilities there may be. We are continuing to follow up on that in terms of an investigation as to what actually happened, and that is ongoing. The bottom line is you will have all the facts as to what may have happened and what other vulnerabilities may need to be addressed, but we are moving forward in concert with the catering company and the airport on that.

Senator COLLINS. Could you explain to the Committee what kind of vetting TSA does of airport employees and others who have access to airplanes but are not passengers?

Mr. PISTOLE. Yes. There is a series of background checks and a fairly robust system in place to assess whether anybody who wants access to either the sterile area of the airport or even the vendors who work in the non-sterile area, and so one of the first checks, obviously, to do is to make sure they are not on some type of terrorist watch list. So that is the first step, obviously. A criminal background check is also done, and then we do vetting that is recurrent for all those, especially those who have that additional access to the sterile area.

We work closely with the companies and the airports for all 450 airports around the country to determine from a risk mitigation perspective, do they see any vulnerabilities in their employees, and then based on what the U.S. Government knows, both within TSA and obviously FBI background checks and the U.S. intelligence community, are there those who may pose a problem.

The challenge comes, frankly, from the clean skins, those who have no criminal background. They have not come up on a terrorist watch list in any way. So that is the challenge that we are presented. And so we also include random and unpredictable security checks both for the catering companies, for example, and for the employees. So we will do random surprise checks, if you will, on an unpredictable basis so terrorists cannot game that system. But it is clearly something that we focus on.

Senator COLLINS. I would like to now switch to the issue of cargo security in the final time that I have left, now that our Chairman, the true Chairman, has joined us. As you may recall, at a hearing that we held in November of last year, I asked you the question that if our government had not received the intelligence tip about explosives hidden in air cargo that was shipped to Yemen, would our current security systems have detected those package bombs, and you very candidly replied that, in your professional opinion, we have not. Could you bring us up to date on what has been done since that time so that we have better screening in place for cargo? We are always going to need intelligence information. That is absolutely critical and it is part of the layered approach to security. But it does worry me that if not for the intelligence tip, these explosives would have made it to their destination, most likely.

Mr. PISTOLE. Thank you, Senator. A great deal has been done, both by the U.S. Government, foreign governments, foreign carriers, cargo carriers, and the International Civil Aviation Organiza-

tion, along with the National Maritime Organization, the World Customs Organization, and the Universal Postal Union, all those groups working together. As you may recall, I was in Sana'a, Yemen, 5 days after this took place to work with the Yemeni authorities, but the day that the intelligence came in, I immediately issued a Security Directive Emergency Amendment that put a ground stop on any cargo coming out of Yemen, of course, as a first step.

What we have done, I believe, very collaboratively is work with industry to assess from a very pragmatic standpoint, what can you do today, what can you do in the short term, mid-term, and long term in working with us? I mean, we can issue regulations day in, day out. The question is, what can they practically do that does not put a halt to the global supply chain, which was significantly impacted when I issued those Security Directive Emergency Amendments?

So what we have done is work with industry to establish standards well beyond—much more rigorous than ours that addresses risk mitigation from a business perspective in addition to the government's perspective. And so, as you know, 100 percent of all cargo coming in on passenger planes from overseas is now screened. All high-risk cargo is screened. And we are working with industry as to the other portions that as we divide, and we work very closely with Customs and Border Protection, their Advance Targeting System, to say there are categories of known shippers and known shipments. For those that are in the unknown category, we need to apply additional scrutiny, and have that applied before it comes to the United States.

So that is what we are working through with carriers around the world, frankly. There are 20 countries that account for 80 percent of all the cargo coming into the U.S. We are working with countries on national cargo security programs. We have already recognized several of those and look to recognize another handful of those here in the not-too-distant future. So a number of steps have been taken.

Senator COLLINS. That is good to hear. GAO, as you know, has been critical that there are still problems with screening palletized cargo and that is a scenario that we are going to need to work on.

I want to turn the hearing back over to the Chairman, but tell the Chairman that Mr. Pistole brought out in his public testimony that the TSA is still capturing four to five guns per day as part of its screening of carry-on luggage and passengers, and he mentioned that just yesterday, the total was six, and one of those guns was at Bradley International Airport, and it was a fully-loaded gun.

So I think that is a very good reminder to us that there still is a need for screening.

OPENING STATEMENT OF SENATOR LIEBERMAN

Chairman LIEBERMAN [presiding.] Thanks, Senator Collins. First, apologies to you, Mr. Pistole. I had to be on the floor when it convened at 9:30, and thanks to Senator Collins. I was just thinking about who is the chairman. I said it has been a real pleasure to work with Senator Collins here, regardless of who was in the majority or minority, and I said before that all that would change in

this session would be the titles we had, so I appreciate her holding the gavel and bringing the hearing to order.

And I agree with what she just said. I know that a lot of people are taking their shoes off, taking their coats off, going through the lines who say, well, this is a nuisance, for what? But when you tell us and the American people that an average of four or five weapons are found every day at airports around the country, it reminds us why.

Incidentally, I hasten to say that a traveler can carry a weapon in a checked bag so long as it is declared and checked, but these are people who are boarding the plane with a weapon in their luggage, four or five every day. So thanks for what you and your folks are doing.

The rule of our Committee is that the first Senator to arrive goes first, and I think the Chairman ought to apply that rule to himself, so I am going to call on Senator Paul, and then I will come after him.

OPENING STATEMENT OF SENATOR PAUL

Senator PAUL. Thank you for your testimony, Mr. Pistole. Does the TSA examine flight manifests?

Mr. PISTOLE. Yes.

Senator PAUL. So when people come through, you have already looked at whoever is flying that day? Someone has looked at that?

Mr. PISTOLE. Yes. It is under our Secure Flight Program.

Senator PAUL. So there are specific searches then targeted toward someone you have looked at on the flight manifest and determined if they may need extra scrutiny?

Mr. PISTOLE. Yes. That is the whole basis of our watch list; it is predicated on knowing who is coming. These are individuals coming to the United States, or flying from the United States. So I start every day with an intelligence briefing that looks out 72 hours in advance to say, who are those individuals who are known as selectees on terrorist watch lists, where there is some derogatory information about them, or clearly the no-flys who may want to fly but will not be allowed to fly, either from the last point of departure to the United States or in the United States.

Senator PAUL. I was just thinking more of people who have been to Yemen three times and Somalia twice and they are not on your watch list, but you might want to spend a little more time with them.

Mr. PISTOLE. Yes.

Senator PAUL. That kind of screening is occurring, also?

Mr. PISTOLE. Yes, and I would be glad to go into some more detail in a closed setting, Senator, in terms of some of the work that we do with the intelligence community.

Senator PAUL. I would just like to know that it is occurring in general terms.

Mr. PISTOLE. Yes.

Senator PAUL. If you fly from Islamabad into Kennedy Airport and then you are going to fly on to Chicago, do you go back through any screening or are you just relying on what happened in Islamabad?

Mr. PISTOLE. No. You go back through additional screening here.

Senator PAUL. You do go back?

Mr. PISTOLE. Yes.

Senator PAUL. So you go back out of the secure area when you have an international flight, and then you come back through the TSA screening?

Mr. PISTOLE. Yes. If you are talking about transiting from one point in the United States to another?

Senator PAUL. Yes.

Mr. PISTOLE. Yes, clearly, the enabling legislation requires us to screen every passenger here in the United States.

Senator PAUL. And with regard to setting up a frequent traveler program, you say there are a couple of airports we are doing it in now?

Mr. PISTOLE. Four right now, Senator, right.

Senator PAUL. And what is the plan for expanding that program?

Mr. PISTOLE. We are working very closely with both the airlines and the airports. I have met with and talked to two airline CEOs in the last 2 weeks who are very interested, and so right now, we are doing it with American and Delta and we are in four of their key airports. So the goal is to, as quickly that we can do it in an efficient way, expand that with airlines and other airports, and so, clearly, there will be some more airports added in the next several months, but more so as we get into 2012.

Senator PAUL. Right. Nashville Airport is not one of those, is it, because I have noticed there are pilots going through a separate line now.

Mr. PISTOLE. Yes. As part of the Known Crew Member Program——

Senator PAUL. That is a separate program——

Mr. PISTOLE [continuing]. That is a separate part of the Risk-Based Security Initiative, separate from and apart from passengers. We have the pilots who, of course, are the most trusted persons on there. Actually, we are doing that at seven airports, but as I mentioned, we have had over—well, it is approximately 80,000 pilots have gone through on this expedited screening process.

Senator PAUL. But it is going to be on an airport-by-airport basis, is how it works?

Mr. PISTOLE. Yes, it is, simply because of the checkpoint configuration layout and if there is an area for either a dedicated lane or near the exit lane or something that we can configure for it. But it is in close association with the Pilots Association and ATA, who are doing all this—at no taxpayer expense, I would add.

Senator PAUL. I would just encourage that we continue to expand this, that it is long overdue——

Mr. PISTOLE. Thank you, Senator.

Senator PAUL [continuing]. And that the smaller we make the haystack of what we are looking in, the easier your job is to find people——

Mr. PISTOLE. Agreed.

Senator PAUL [continuing]. And that involves more of making priority and targeting folks who are more risk to us. And anything we can do to have fewer pat-downs of 6-year-old girls—in fact, I do not really think there is any reason why we should be doing that—we need to get to that point. With an adult, when an adult goes

through and the image is blurred, can the adult request to go back through again?

Mr. PISTOLE. Our policy has not been that. That is what we changed with children, simply because——

Senator PAUL. I would change it with adults, too. Ninety-nine-point-nine percent of us are not terrorists. Let us go back through the machine rather than get a pat-down. You will get rid of a lot of the anger an animosity toward the TSA and toward what you are doing and give us a little more dignity when we travel. Just let us go back through the screener again. People do not want to have a pat-down.

Mr. PISTOLE. Yes. I will take that back, Senator.

Senator PAUL. We are made to feel like criminals and we do not want to be made to feel like criminals when we fly on a plane.

Mr. PISTOLE. Obviously, the only down side is it slows down the line and then people—you obviously want to keep moving along, and so it is a——

Senator PAUL. I am not sure it slows it down that much just to send them back through, particularly if they give them a choice, they can do a pat-down or a walk back through. But I think what happens is when you ask any questions, you are treated like you are guilty of some crime and you are treated roughly and it is, like, do anything, ask any questions, and we will pat you down more, or we will be more invasive. That is sort of what you get sometimes as you go through the airport. But I think we need to try to continue to do what we can to isolate and target who could attack us and to try to make it easier on those who are not going to attack us, which is recognizably 99.99 percent of us are not terrorists. So we need to figure out how to get them through in an expedited fashion and in the most dignified way. Thank you.

Mr. PISTOLE. Thank you, Senator. That is exactly what this whole Risk-Based Security Initiative is designed to do, so thank you.

Chairman LIEBERMAN. Thanks, Senator Paul.

Thank you, Administrator Pistole, for all the good work that you are doing. I am so struck by the example of the four to five weapons a day that are seized in the lines and I think it is very important, to the extent that you are able without jeopardizing security to regularly announce to the public, generally speaking, what you are finding because there is a level of impatience. I think people have resigned themselves to it, but the average person going through the line—I speak for myself—does not see somebody get stopped with a weapon and it is very important to remind people why we ask them to go through this, which is for their own security.

I know you mentioned in your opening statement the ability of the whole body imaging machines to actually find a Nicorette in somebody's back pocket. I know from having talked to you there have been occasions when you found things concealed on a person which would not show up in a metallic scanner that could be very dangerous to the other people on the plane. So I do not know if you want to respond at all to that——

Mr. PISTOLE. Well, I appreciate it, Mr. Chairman. It is a good reminder. We do post some things on our TSA Web site and we have a fairly active blog that people interact with us on.

Chairman LIEBERMAN. Right.

Mr. PISTOLE. One of the keys is not providing too much detail so the terrorists can go to school on what are the detection capabilities and not, but clearly, just the fact that we are getting four to five guns every day indicates that there are people who are not focused on the security protocols.

Chairman LIEBERMAN. Good enough. Thank you.

Yesterday, as you probably know, ProPublica, an independent news reporting organization, in conjunction with Public Broadcasting, published an investigative report on backscatter machines, one that has become acceptable to use in airports, but the article summarizes health concerns raised by experts over the past 15 years about these machines. I wanted to give you an opportunity, because I know this has been in the news the last 24 hours, if you choose to respond to these concerns at this time.

Mr. PISTOLE. Yes. Thank you, Mr. Chairman. I did see the article yesterday and it does contain a lot of information. I am not sure all of it is accurate from the standpoint of documenting all the different perspectives. Clearly, it is an issue that we have looked at and continue to look at and work with safety and health officials to ensure that these backscatter invasive technology machines are as absolutely safe as can be, and all the independent studies that we have had done indicate that they are well below any of the minimum dosages recommended.

I take Senator Collins's recommendation to heart, to have DHS do an independent study, and we will take that up and do that because of these lingering concerns about any additional exposure. Of course, what the scientific studies that we have seen indicate is that it is about the same amount of radiation as approximately 3 minutes of flight at elevation, just naturally occurring radiation. It is one-one-thousandth of a time, for example, of a chest X-ray. But that being said, I am concerned that there is a perception that they are not as safe as could be, and since we are using different technology, that would be millimeter wave, that does not have that same perspective, I will take that back and we will conduct another—an independent study to address that.

Chairman LIEBERMAN. Thank you.

Let me ask you about another matter that has been in the news. I am sure you know that over the weekend, during the Winter Storm Alfred, there was a nightmarish series of events at Bradley Airport. To make a long story short, I and others have been asking questions of Jet Blue, the FAA, and Bradley Airport. The reality was that a lot of planes could not land where they were heading. They were running out of fuel and they were being diverted to three airports, one of which was Bradley Airport, which became very crowded and all the gates were full. They were making judgments about keeping the runways open.

In the worst cases, I am sure, passengers on that Jet Blue plane stayed 7 hours, no water, no food, no bathrooms working, really a nightmare. And finally, Jet Blue was able to get a bus to go out

to take the passengers off, and the airline may well be subject to considerable fines as a result of all that.

That is not directly in TSA's area of responsibility, but I did want to ask whether you might have contingency plans, or should, for dealing with an unexpected influx of passengers and maintaining security at an airport when flights are unexpectedly diverted from another airport to that airport.

Mr. PISTOLE. Thank you, Chairman. We do, within TSA, have contingency plans. Obviously, with a little bit more head's up, for example, if there is a hurricane, something like that coming in, we have a National Deployment Force that we can actually move individuals on an expedited basis, within hours, to an affected area that may need additional security regimen, either for the passengers, pilots, crew, or the workers.

Chairman LIEBERMAN. Yes.

Mr. PISTOLE. So we do have that capability and we use that. We used that in Hurricane Irene. But it is something that was started going back to Hurricane Katrina, which actually is where it stemmed from. So, yes, we do have that.

Chairman LIEBERMAN. That may preface an answer to my next question. It happened that one of the diverted flights to Bradley Airport was an international flight, and it raised an interesting question and I want to ask Customs and Border Protection about it. If the passengers on that international flight were forced to stay on the plane so long that it was just humanely impossible and they had to be taken off the plane and brought into the Bradley Airport, which of course, has a sizeable contingent of TSA personnel—whether there is any way TSA and CBP can work together in those unusual circumstances to process passengers more quickly so that they are not forced to stay on the plane for an enormous amount of time simply because they happen to be on an international flight?

Mr. PISTOLE. I know there are some provisions. I do not know the details, so I would have to look into that and get back with you and the Committee on that. For example, if it is a situation where international travelers are trying to get out of the country——

Chairman LIEBERMAN. Right.

Mr. PISTOLE [continuing]. They have already been processed. If it is a matter of them then being reprocessed, and because their flight is not going to depart, there are some options, but they are, frankly, somewhat limited if there is not a good CBP presence there.

Chairman LIEBERMAN. Yes. I mean, Bradley Airport is an international airport, but all of the scheduled international arrivals currently originate from countries with CBP pre-clearance stations, so there may not be adequate clearance to handle some unexpected international arrivals—it may be a rare circumstance. On the other hand, we have had some extreme weather lately, so I just ask you to think about that.

Mr. PISTOLE. I will follow up with Commissioner Alan Bersin on that and to see what the options may be.

Chairman LIEBERMAN. OK. Thanks. My time is up. Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, for holding this hearing on "The Next Wave in Aviation Security."

Mr. Chairman, because Hawaii is located 2,500 miles from the mainland, we have, of course, unique transportation needs. Hawaii residents and our many visitors rely heavily on air transportation when traveling between islands and also to the mainland or even abroad. Although protecting the public is our primary goal, we must ensure that security procedures and technologies safeguard privacy rights and are not so burdensome that they discourage air travel.

I applaud the Federal employees who have worked tirelessly to secure our commercial aviation system since September 11, 2001. As we approach the busy holiday travel season, I hope this hearing will allow us to review whether the workforce has the tools they need to meet today's security challenges.

Administrator Pistole, your testimony mentioned that TSA is in the first phase of the expedited passenger screening pilot. I understand that Honolulu Airport and Hawaiian Airlines are being considered for the second phase of the pilot. In Hawaii, many people who take frequent short flights between islands could benefit from the expedited security procedures. How are the decisions being made about which additional airports and airlines will be selected for the second phase of the pilot, and when will those selections be announced?

Mr. PISTOLE. Well, thank you, Senator Akaka, and thank you for your support for Federal employees. Clearly, the goal is to move out as quickly and efficiently as possible. There are a number of variables that we are working through and those include things such as the airlines' capability, their information technology systems. Because the way this expedited traveler, if you want, TSA Pre-Check works is that we take information that is embedded on the bar code of the boarding pass, which the airlines, of course, produce, and so it shows up in that bar code as the person is a known or trusted traveler, if you will. Several airlines are going through mergers right now and they are waiting until those systems are merged as opposed to having disparate systems that do not talk and then trying to merge those into a new one. So those will be after the first of the year. So that is one criteria. Is the airline ready, capable, and all that.

The second is the airports themselves, and the configuration of the checkpoint is a key aspect. One of the goals of this is to have a dedicated lane for those known, trusted frequent travelers, such as in Global Entry or these elite tiers and others that we will look at down the road, so they can go to a dedicated lane, they can be identified through that bar code on the boarding pass, and then we can have a separate screening lane for them where they keep a light jacket on, they keep a belt on, they keep their shoes on, they keep their laptop in their briefcase, keep their liquids and aerosol gels in their carry-on bags, and again, keeping random and unpredictable checks as part of that.

So to directly answer the question, there are a number of airports and airlines that we are working with to try to get to that point, so I want to manage expectations as best I can to say there

have been no decisions made. I am waiting on a presentation for that second round, if you will. I will say that I met with the CEO of one of the major airlines going through a merger here the week before last and they are committed to doing it in the first quarter of 2012, and so we will use one of the very largest airports in the country as the basis for that airline, that merged airline, probably in the February-March time frame. So as soon as we get some additional information, I will get back with you on that.

Senator AKAKA. Thank you so much.

Administrator Pistole, I applaud TSA's increased use of Automated Target Recognition software, so that whole-body scanners no longer generate sensitive images of passengers' bodies. However, I am concerned that the backscatter machines, which are not currently compatible with the ATR, are still used in many airports, including some in Hawaii. Does TSA plan to implement the privacy-enhancing ATR feature for all whole-body scanners, and what is the time line for doing so?

Mr. PISTOLE. Yes, Senator. In fact, we just were approved to acquire 300 more additional AIT machines and all of those will have that Automatic Target Recognition. So no new acquisitions will be without that privacy feature built in. We should know sometime this month from the manufacturer of the backscatter whether their technology upgrades, if you will, are successful in terms of the depiction through the ATR rather than through the traditional means. But any new acquisition will have that privacy filter of the ATR as part of that.

Senator AKAKA. As you know, the APEC summit will be held in Honolulu, Hawaii, next week. The high-profile event will feature President Obama and his fellow APEC leaders from the Asian region. I recently met with the security steering committee and toured the command center and event sites. I was very impressed by the planning. Would you please discuss TSA's role in securing the safe travel of the 20,000 dignitaries and guests flying to Hawaii.

Mr. PISTOLE. Thank you, Senator. Obviously, the U.S. Secret Service, the Diplomatic Security Service, and the State Department have the lead as far as the dignitaries themselves and their entourage. It is our responsibility, honestly, to ensure that everybody traveling to the summit, other passengers, other attendees, and things, have been thoroughly screened, whether they are coming from the mainland or from those last points of departure to the United States that have to meet our standards. So that is our responsibility, and then, of course, on the departure, all those people will go through the TSA security screening.

Senator AKAKA. Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Akaka. Senator Pryor.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Thank you, Mr. Chairman, and thank you, Mr. Pistole, for being here.

Let me start by asking about a March 2010 DHS Inspector General report entitled, "Transportation Security Administration's Acquisition of Support Services Contracts."

It is DHS IG Report 10–72. The DHS IG made some recommendations in the report, and I am curious about whether your agency has made the changes and is now complying with the recommendations in that report.

Mr. PISTOLE. Senator, I think I am going to have to be refreshed on the specifics of that particular report——

Senator PRYOR. The three main recommendations that I am concerned about are: First, a review of inherently governmental functions as part of contract administration. Second, to establish evaluation factors and a review process for requirements identified in the statements of work. And third, assign dedicated, trained, and certified contracting officers, technical representatives to manage and oversee the contract administration function.

Mr. PISTOLE. Thank you, Senator. I appreciate that refresher. So we have taken a number of steps as it relates to support services and contractors, and working within the framework of the Department of Homeland Security overall, we have conducted a review of all of our contractor services and, frankly, eliminated a number of positions. A number of other positions that were deemed inherently governmental services were converted to Federal employees. So the idea is to achieve greater efficiencies in our use of contractor dollars and services.

As to the specifics of the acquisition, I think we identified some areas of improvement, or that were identified, some areas of improvement that we have implemented. I would have to get back to you on some of the specifics.

Senator PRYOR. When you talk about efficiencies, does that mean savings?

Mr. PISTOLE. Savings, yes.

Senator PRYOR. And do you have a dollar figure on how much you are able to save?

Mr. PISTOLE. I do not offhand. I will be glad to get back with you on that. I would also say that as a part of an internal initiative that I started 6 months ago to look at efficiencies that we could achieve within the agency beyond any IG, GAO recommendation——

Senator PRYOR. Right.

Mr. PISTOLE [continuing]. We have come up with a number of opportunities to create efficiencies, savings, and cost avoidance and things that are all important to us and still provide the same critical security services. It is largely a headquarter-focused efficiency review, so, for example, I have put a freeze on hiring in most positions. I have required additional information about anybody who is at a mid- or senior-level supervisor position to make sure that they have requisite subordinates that they are supervising, merging some IT functions, and doing some other things internally.

Additionally, from the field perspective, I recently implemented a decision to change our overall structure, where we had 12 area directors that oversaw the work of the 120 Federal Security Directors for the 450 airports, and I reduced that from 12 down to six Regional Directors to create some additional efficiencies in that regard.

Senator PRYOR. That is good. I would like to get more on that in terms of how much you think you can save and how those efficiencies will work. That would be great.

And the next question would be whether, in the past, TSA has invested in technology that did not yield the predicted results, such as puffer machines. So I am curious about what criteria you all use as you are evaluating technology, and then how you measure whether the technology is going to achieve the anticipated goals that you are trying to achieve.

Mr. PISTOLE. Yes, thank you, Senator. The first criteria is what does intelligence tell us about how the terrorists are trying to hurt us, and so with that as a starting point, then we work with industry to say, what detection capabilities do you have currently and what are you working on that either others are incentivizing worldwide because if somebody comes up with a gold standard, it is a very important and valuable commodity. So we use those two criteria and then always push industry to improve the detection capabilities.

For example, on the AIT, we are working very closely with industry. The GAO and IG both have reports coming out about some of the detection capabilities, and there is a distinction between what is the capability of the machine vice what may be seen as performance testing. So covert testing versus performance testing, and so we always try to make that distinction.

But it has to be intelligence-driven, risk-based, and then to make sure that it is properly tested and validated, not only in the lab, as happened with those puffer machines, but then in the airport environment itself, which did not happen. And so after the puffer machine issue, we actually created a Transportation Security Integration Facility, which I know some staffers and some Members of Congress have visited. It is just on the South side of the Reagan Airport in Virginia. I would like to invite all Members and staffers to come out and tour where we test each new piece of technology in an airport environment to make sure that it works not only properly, but rigorously and all those standards that—not just in the lab setting.

Senator PRYOR. It sounds like a lot of that has to do with training and to making sure the officers are properly trained on the machines.

Mr. PISTOLE. That is a good point.

Senator PRYOR. Let me ask you another question that relates to training. You are expanding your Behavior Detection Pilot Program and I would like to know more about that. It seems common sense, that behavior obviously would be a strong indicator, but does it accommodate cultural differences, language barriers, and physical and mental disabilities? How do you balance those needs, compared to trying to single out erroneous folks, who for whatever reason TSA is picking up erroneously?

Mr. PISTOLE. Right. So, clearly, training is a key aspect of this expanded Behavior Detection Initiative that we are trying, and it is a proof of concept that we are doing in Boston and Detroit right now, and I want to get the data from those two airports before I make any decision whether to expand it or not. But we have, of course, our core Behavior Detection Officers that we have been

using for several years now and we have taken those individuals who showed the most aptitude and give them additional training based on some form behavior detection models, and those individuals then engage in just a simple question and answer with passengers in these two airports to make some assessments and judgments as to whether that person poses any additional risk.

Now, in Boston, we have had over 150,000 people go through and, just again, answer these basic questions, and we have had probably a dozen or so people who were referred to law enforcement because of their response and it turned out some of these individuals had outstanding warrants for them. Some were illegal immigrants. So they are not necessarily TSA security issues, but there was something about the person that we needed to resolve why are they acting nervously or strangely or whatever.

So as I get that additional information, I will look forward to reporting back to the Committee and say, here is what we are finding and here is what I think would be the best thing to do moving forward, recognizing that it is simply one layer of security, that I do not want to have a single point of failure in any of our layers. If this helps us identify that one putative terrorist, then I would like to use that.

Senator PRYOR. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Pryor.

The late, great Ted Kennedy—I watched him in the Armed Services Committee and we have a rule, first come, first called on, so he would arrive a minute or two before the hearing convened. The Chairman would gavel it down, and then he would disappear. And, like, 30 seconds before it came his turn, he would reappear. So he was maximizing his time.

Administrator Pistole, I thank you. We have a second panel and I think it is probably best that we go on. You are doing a great job. I think you certainly convinced me that all the effort we are making continues on a daily basis to be necessary, and I cannot stress enough, and I know I speak for Senator Collins, your people are finding four to five weapons every day, not in checked bags where they are legal, but people going on the plane. And just think about what could be done to the other passengers. So what the TSA officers are doing is for the protection of the general public.

Obviously, we want you—and I know you want—to do your mission in the most cost effective way that you possibly can and in the most technologically progressive and imaginative way that you can. But we thank you for what you are doing. It has, just point blank, made the American people safer than we would otherwise be.

Some of us may have questions for you that we will submit which we did not get a chance to ask you today and ask for your answers. Thank you very much.

Mr. PISTOLE. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Have a good day.

Mr. PISTOLE. Thank you.

Chairman LIEBERMAN. We will call the second panel, which is Roger Dow, President and Chief Executive Officer of the U.S. Travel Association; Kenneth Dunlap, Global Director of Security and Travel Facilitation at the International Air Transport Association;

and Charles M. Barclay, President of the American Association of Airport Executives.

Thank you all, gentlemen, for being here. We look forward to your testimony. Each of you has unique experience and perspective to add to this discussion. As you just heard me say, I am grateful for the work that TSA does, but as somebody said in another capacity, this is a journey without a destination point. In other words, we are just going to have to keep getting better and better and better as time goes on.

So let us begin with Mr. Dow.

TESTIMONY OF ROGER J. DOW,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, U.S. TRAVEL ASSOCIATION

Mr. DOW. Thank you. Chairman Lieberman, Ranking Member Collins, and Senator Moran, thank you very much for this opportunity to testify.

Senator Lieberman, first of all, we want to thank you for your dedication as you are about to retire. You have pursued bipartisan support for aviation security and we are going to miss you.

So thank you very much.

Chairman LIEBERMAN. Thank you.

Mr. DOW. U.S. Travel is a nonprofit organization that represents every sector of the $1.8 trillion travel industry, which employs one in nine Americans. Our mission is simple: To increase travel to and within the United States.

As you all know, travel is a very powerful engine for increasing economic growth and improving our economy and jobs. Just in Connecticut, 62,000 Americans work in the industry, and travel generates $8.8 billion in revenue and $1.4 billion in taxes. In Maine, 30,000 citizens work in our industry, and travel generates $2.7 billion in revenue and $334 million in taxes. But in every city and State, travelers support the salaries of policemen, firemen, and teachers, all around America. And I think it is also important to point out that travel attracts private sector investment, whether it be airports, hotels, convention centers, or attractions, that really help the communities build.

When we talk about aviation security, we often talk in terms of terrorism, personal privacy, and technology, and less attention gets paid to the economic damage that is inflicted by the current inefficiency in our passenger screening process. For the travel community, which supports urban and rural communities, inefficient screening really causes staggering costs to the economy, hampering job creation, hampering growth, and the data suggests the problem is actually getting worse.

A 2008 survey of air travelers showed that of the people that take more than one flight a year, 28 percent said they avoided a flight because of the door-to-door hassle of getting through the airport and delays, etc. That resulted in 41 million flights not taken, or $26 billion in lost spending to our U.S. economy and $4 billion in lost taxes.

You compare that $26 billion loss with a 2010 survey that was conducted by Consumer Research and asked travelers, if you knew

[1] The prepared statement of Mr. Dow appears in the Appendix on page 1235.

that you had a predictable screening system, would you take more flights. Respondents said they would take two or three more flights per year, which is $85 billion in revenue and would support 900,000 jobs.

The costs of TSA's budget are ballooning at a time when we are trying to find fiscally responsible ways of cutting costs in government. For example, in 2004, 618 million people went through an airport. In 2010, it was 623 million, a scant one percent improvement of the numbers, but yet during the same time period, TSA's budget increased 68 percent. This trend cannot continue or security screening is going to fall in on itself on sheer costs and manpower. The FAA is predicting that in 10 years we will have a billion travelers. So just think if the costs keep raising at that rate, what would happen.

Beyond the empirical numbers, there is other evidence. You all, as Senator Collins said, travel every single week. You see the inefficiencies and the need for reform in the security system and it could really stimulate economic growth. Our current system, while it reduces threats and ensures passengers' safety, has also been inefficient and there is a huge hassle factor.

We brought together in 2009, a blue ribbon panel of bipartisan aviation security experts and travel industry experts. It was chaired by former Homeland Security Secretary Tom Ridge, former Congressman Jim Turner, and Sam Gilliland of Sabre. The goal of the panel was to review the present process and recommend some reforms in creating a more efficient and secure and travel-focused system. They had over 20 meetings and we issued the report called "A Better Way,"[1] and you have a copy of it, which presents a comprehensive review of what could be done.

The report lays out a checklist with 14 recommendations so the Congress and TSA could really have a road map for creating a secure and efficient system. I am going to focus on three of those recommendations in my remarks. First, we must create a risk-based trusted travel program, which Administrator Pistole spoke about. Second, we must take steps to decrease the number of carry-on bags. And third, TSA must reconstitute the Aviation Security Advisory Committee.

Let us go to the first one. The blue ribbon panel said they wanted Congress and TSA to create a risk-based system, and the need for that is very clear. The current one-size-fits-all screening really does not meet the needs of the traveling public. Currently, travelers have no choice in how the system works. We have to have security, of course, but in our view, a trusted traveler program would allow travelers to opt in voluntarily and provide background information to qualify for a predictable expedited screening system as long as they meet certain criteria that are established for these low-risk passengers, which would be just about everybody in this room, if you think about it.

The blue ribbon panel recommended three elements of a trusted traveler program. First, a trusted traveler program must be secure and accessible program that encourages reverification and encourages a large number of enrollees, not just a small number. Having

[1] The report referenced by Mr. Dow appears in the Appendix on page 1241.

a dedicated screening lane for trusted travelers, as Administrator Pistole said, is important. And a confirmation process ensures that these enrollees are able to use those lanes is also important. And third, the program should have a screening process that provides efficiency, security benefits, and an acceptable level of predictivity. We strongly believe that those three elements can take place.

Not long after our release, our team met with Administrator Pistole's team to review these recommendations and get their feedback. At that meeting, we learned of several initiatives that are underway at TSA to create a risk-based, intelligence-based system. For example, Administrator Pistole and TSA are creating the Pre-Check program. I applaud him for his vision, his leadership, and undertaking an effort to launch Pre-Check, which is an important first step. Pre-Check is one of the critical reforms that is very important. I also applaud all of you for taking an interest in this area and hope that we can work with you to begin to oversee the implementation of a process that is efficient, yet still provides great security.

As the Administrator mentioned, they recently started Pre-Check and it is going forward with putting passengers in that program who qualify through their airline or through the CBP program, Global Entry. Pre-Check allows people to share information from their frequent traveler program, whether it is Delta or American Airlines, that qualifies them for expidited screening.

What we basically would like to see for this to succeed would be for Pre-Check to allow more people to get into the program, allows people to take their information from multiple airlines, not just two airlines, and also use other methods of enrollment, such as commercial data, criminal history, and the private registered traveler programs that other people are administrating.

The second area of improvement is to have dedicated security lanes. We have talked about that. And also, as Administrator Pistole said, have random security, which is very important, but if you are randomly pulled out, you should still be expedited and have predictability.

The next key area of reform we want to assess is to have passengers be able to check one bag at no additional cost. Now, we are not saying at no cost to the passenger. The airline should be able to put in their standard fee for their airline ticket a cost for that bag. But if we could reduce the number of bags, we would reduce those guns that you talked about. We would reduce the hassle and the ability to quickly go through the checkpoint. The *New York Times* said 59 million more bags came through TSA checkpoints in the past year. TSA estimates an increse of 87 million carry-on bags in the past year and 29 million more bags next year. So if we could get one bag per passenger, people would check them and it would improve the system greatly.

And the last thing I would like to highlight today is the reinstatement of the Aviation Security Advisory Committee. This has been in place for two decades with the FAA and TSA, but it really brought in a broad base of people to advise the government. But unfortunately, as we have seen, since 2006, the ASAC has not met. Therefore, you cut off valuable input from the private sector, from the travel community, etc. In July 2011, the TSA Administrator an-

nounced they are going to reconvene that committee and we think that is great and we would hope that we would have the travel community involved so we can have the input of the travelers because we do not believe that having great security and great customer service and an efficient system are mutually exclusive. You can have both.

So we are asking your support to allow us to work with you to have a system that is secure, has trusted travelers, has a way that we can reduce the number of bags going through the system, and that we reinstate the broad spectrum of people providing advice to TSA.

Thanks for what you do. We appreciate your support.

Chairman LIEBERMAN. Thanks, Mr. Dow, for an excellent opening statement and for your kind words.

Mr. DOW. Thank you.

Chairman LIEBERMAN. Next will be Kenneth Dunlap on behalf of the International Air Transport Association.

TESTIMONY OF KENNETH J. DUNLAP,[1] GLOBAL DIRECTOR, SECURITY AND TRAVEL FACILITATION, INTERNATIONAL AIR TRANSPORT ASSOCIATION

Mr. DUNLAP. Chairman Lieberman, Senator Collins, and distinguished Members of the Committee, thank you very much for this opportunity to testify at this hearing.

The International Air Transport Association, appreciates the leadership of the Senate in addressing this critical issue. It is our hope that today's hearing accelerates the much needed dialogue on the future of passenger screening post-9/11 in the United States.

IATA and our 230 U.S. and foreign member airlines have a vision of future passenger screening that is based on a paradigm shift in the principles behind checkpoint operations. We believe next-generation checkpoints must focus on looking for bad people and not just bad things, and I would ask that you consider for a moment our vision of an effective airport checkpoint. Security is enhanced with higher probabilities of detection. Babies and children with names similar to adults on the no-fly list pass through screening uneventfully. Harmless objects, such as toenail scissors and nail clippers, do not trigger alarms.

In this scenario, the airport security checkpoint is no longer a stand-alone line of defense against terrorism but rather part of an integrated system that uses risk-based analysis as well as advanced screening technology to improve security and the travel experience for the passenger. We call this vision, the checkpoint of the future, and many of the key components are available today. But let me stress, this is a vision, this is not the vision of moving forward, and we certainly want to encourage a dialogue on what the next future checkpoint should look like.

I think the obvious question is, why develop a future checkpoint? First, as we have heard, aviation remains a target, and this was demonstrated by the December 2009 attempted bombing of a Northwest Airlines flight bound for Detroit.

[1] The prepared statement of Mr. Dunlap appears in the Appendix on page 1278.

Second, air travel is forecast to continue growing and today's checkpoints are showing their age. IATA expects an additional 90 million passengers will travel within North America between now and 2014, and 659 million new passengers will travel in the entire world. Our long-range projections are that by 2050, as many as 16 billion people will fly annually. But the evidence shows that the throughput of today's checkpoints is decreasing. Our systems just cannot handle the traffic. At some places across the globe, we have seen a drop in throughput by as much as 50 percent in the last 2 years.

And third, the aviation security system needs to maintain the confidence of the traveling public, and unfortunately, the signs of discontent are growing. Passengers are becoming increasingly vocal about the inconvenience of security measures and the threats to their personal privacy. But let me stop and let me be clear about one thing. We have good systems and the flying public is safe. But we also need a confident public that trusts the authorities. If you have good systems combined with distrustful passengers, you create a toxic combination and a less secure system.

So what lessons have we learned in the past decade concerning passenger screening? First, dropping new technology into an old checkpoint just will not work. That is akin to placing a new radio in an old car and saying you have a new car. Essentially, you just still have that same old car.

Second, object finding has served us well, but it does not represent the future. If we have learned anything in the last decade, it is that a passenger with toenail clippers is not automatically a threat to aviation. Alternatively, if you find toenail clippers, you have not necessarily found a terrorist.

And third, one-size-fits-all screening has outlived its usefulness. Over 2.8 billion passengers are screened per year and we cannot continue at this pace without using risk-based screening measures. IATA strongly supports Secretary Napolitano and Administrator Pistole's calls for risk-based screening.

So IATA has been working for the last year and a half on developing a more efficient, more effective and relevant passenger screening checkpoint, and let me just spend the last few minutes remaining discussing the core principles and explain how we propose turning these into a checkpoint.

The checkpoint of the future concept described here relies on two basic concepts. The first is the introduction of risk-based screening, using data from travel documents and airline tickets that is already being used by the U.S. Government and other governments for customs and immigration purposes. And let me just stop again and emphasize, this does not involve profiling of passengers of any kind. We are simply proposing that rather than using this data only at the end of a journey for purposes of border control and immigration, we should use it at the beginning of the journey for security purposes.

And the second concept is the use of advanced screening technology to enable a seamless journey through screening lanes without removing items of clothing or unpacking luggage. So, you might ask, what does this look like at an airport? Well, for a passenger arriving at an airport checkpoint, the passenger will biometrically

identify himself or herself and have a brief encounter with a behavior analyst. The passenger is assigned to a lane based on the results of their electronic pre-screening or random selection. The passenger proceeds through the lane and is screened while in motion. Passengers who voluntarily opt into a known traveler program and agree to provide additional information about themselves would proceed through a known traveler lane. Those about whom little is known or those randomly selected would go through an enhanced security lane. But let me emphasize, all passengers are screened to a baseline, and in this concept, no one—no one—gets a free pass.

So where are we and what have we done? IATA has developed a high-level blueprint and a road map. We are working with like-minded associations, manufacturers, academics, and airlines to refine this concept, and this certainly needs to be a global effort. To date, ICAO has endorsed the need for a global effort to study a future checkpoint. Interpol and 12 States have signed statements of principle that we are headed in the right direction.

Now, we certainly expect that in 7 to 10 years, all the necessary components for a walk-through screening process will be available, but we can repurpose and reintegrate existing technology into an intermediate checkpoint. That is possible within the next 2 to 3 years. And this reworked checkpoint uses existing hardware and combines several essential elements of the checkpoint of the future, including passenger data already being used by governments, behavior analysis, and the creation of new screening lanes.

IATA is committed to making air travel safe, secure, and more enjoyable, and in summary, we believe the foundation of the checkpoint of the future should be based on the lessons learned since 9/11 and the next generation checkpoint should use passenger data, use behavior detection, screen passengers based on risk, provide for an uninterrupted journey from curb to aircraft door, and preserve our investment in our existing checkpoints. We will not settle for anything less than a revolution in the way our passengers are treated at the airports.

Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Mr. Dunlap. That was really fascinating. You have helped us to, no pun intended, look over the horizon here, at least in terms of security at the airports, so I have some questions I will ask you when we get to that.

Finally, Charles Barclay on behalf of the American Association of Airport Executives. Thanks very much for being here.

TESTIMONY OF CHARLES M. BARCLAY,[1] PRESIDENT, AMERICAN ASSOCIATION OF AIRPORT EXECUTIVES

Mr. BARCLAY. Thank you, Mr. Chairman, Senator Collins, and Members. It is always a privilege to be here. I am just going to take a very brief time and make two general points from our testimony.

The first is that Airport Executives strongly support risk-based security. We congratulate Administrator Pistole and his team for bringing that concept forward. It is something that is essential for the future, as you have heard.

[1] The prepared statement of Mr. Barclay appears in the Appendix on page 1285.

We support Pre-Check and encourage its expansion. Airports are eager to, as well as airlines, be sponsors of that program in local areas. We would ask the Committee to encourage TSA to move as quickly as they can from the pilot programs into further deployment of Pre-Check.

The rationale behind risk-based security, we think, is pretty simple. You have to look for dangerous people, not just dangerous things, in the future. We have to identify the vast, vast majority of people traveling who are not a threat to the system so we can focus our limited resources on the people we do not get to vet in advance. And then, finally, the resources and facilities. If we continue the current system of treating everyone the same, they are going to be simply overwhelmed by passenger growth. So we have to make changes and modernize.

Risk-based security is not a compromise in our point of view. When you think about the philosophy, a dangerous person with nothing on them that we vet for, that we screen for, is a danger to the system while a person with no bad intent with lots of dangerous things on them is not a threat to the system. So we need a future security system that implements that understanding.

My second general point is that airports are unique partners of TSA. They are all branches of local government, local or State creatures. They all have local police powers and they all have branches, divisions, or special units that have people with precisely the same incentives as the agents of Federal law enforcement.

My point for emphasizing that is that we have today a division of responsibilities. Local governments, airports, and local law enforcement are responsible for things like perimeter security, the front line of employee vetting and credentialing, incident response, and other areas that we mentioned in our testimony. We strongly believe those things should stay with local law enforcement. The TSA should not take over those areas because you do have a partnership between Federal law enforcement and local law enforcement. We need both of them to avoid focusing on each other. You do not want the good guys spending lots of time and energy watching each other as a regulator and a regulated entity.

You want them both pointed outwards looking for bad guys, and we think that is a key element of having a partnership on security between local law enforcement and TSA, as opposed to having the agency take over more areas. TSA has its hands full with vetting and screening both passengers and cargo, and we want to see them do that well. It keeps our commerce moving. It keeps our system moving. We look forward in a future system to being partners with TSA and hope to carry out that mission as well as we can. Both groups will make mistakes. We will both have to learn from those mistakes and get better as time goes on. But local law enforcement and airports are there to be of assistance, and there is no higher priority in their view than the safety of the local citizens they work for.

So thank you and I would be glad to answer any questions I can from our testimony.

Chairman LIEBERMAN. Thanks very much, Mr. Barclay. Very interesting testimony.

All of you, and Administrator Pistole, as well, used the term "risk-based security." Does everybody agree that what we are saying is that risk-based tends to focus on looking for dangerous people as opposed to dangerous things, which is the focus of the current system, right? But I presume that none of you would say that we should stop looking for dangerous things, is that correct?

Mr. DOW. Yes. I think, personally, that we have to look for dangerous things, but there are ways to do that. If you take trusted travelers and they go through a machine that detects explosives, that is fine.

Chairman LIEBERMAN. Right.

Mr. DOW. But the question is how do you make the system much more efficient so you can focus on the dangerous people and the dangerous things.

Chairman LIEBERMAN. Yes. I mean, this is a real challenge, because let us just go to the point of Administrator Pistole's testimony that both Senator Collins and I responded to. So you have an average of four to five guns found in baggage that people are sending through the line to carry on, not check. And I presume most of those are not terrorists. They are, for one reason or another, people who wanted to carry the gun on with them, maybe because it was their sense of how they protect their own security. But, presumably, if you did not have that kind of screening for dangerous things, somebody who was, in fact, a terrorist would be able to carry a weapon on.

So what I am getting at is, and I know it is hard to do everything, and I support moving toward risk-based, which looks for the dangerous people, but we are not at a point where we can ignore looking for dangerous things, are we? Mr. Dunlap.

Mr. DUNLAP. Mr. Chairman, I think that the presumption is everybody does, in fact, get screened——

Chairman LIEBERMAN. Yes.

Mr. DUNLAP [continuing]. So those guns will be found. But in the new paradigm, some people will get screened more, and that if you have the opportunity to do things like enhanced security lanes, you can screen a population of people a little bit more thoroughly.

So if we start with the presumption that there is a baseline, then to address your point, those bad objects are going to be found, as well, but they will not be the entirety of the focus of the checkpoint screening experience, because, again, if you spend your resources on looking for toenail clippers and scissors——

Chairman LIEBERMAN. Right.

Mr. DUNLAP [continuing]. You are not spending enough time looking for IED components.

Chairman LIEBERMAN. No, that is a good approach. In other words, the risk-based is in some sense on top of a more efficient application of the existing system. I mean, I noticed in the vision of the future you have that even the known travelers who have been pre-checked, etc., they go through a metal detector in that walk-through, that particular tunnel.

Go back a little bit, because it is intriguing to look at your vision of the future here. I know you quoted some numbers, but how close are we to that? It looks pretty attractive. I mean, you have three

lines that people walk through. Presumably, that is it. How close are we technologically to that?

Mr. DUNLAP. So, Senator, if you take a look at the intermediate checkpoint that was the last slide depicted——

Chairman LIEBERMAN. Right.

Mr. DUNLAP [continuing]. We are within 2 to 3 years of that.[1] Everything that we need to deploy a more effective security system and a more efficient security system using existing equipment is there today. So we think within about 2 years, we can have that deployed to any airport, and it will use passenger data, which we have today, behavior detection, here today, screening passengers based on risk, we can do it today. And then if you push the future out and you look at the tunnels of technology that we are developing, the one thing that we need is explosives detection that is performed while the person is in motion. That is probably 7 to 10 years on the horizon——

Chairman LIEBERMAN. Right.

Mr. DUNLAP [continuing]. And we certainly cannot do that today. But what we are encouraged is that the manufacturers we are working with are telling us that vision is far closer than what we realize. So, obviously, technology grows exponentially and we think if we have a plan that preserves the current capital investment in our checkpoints, rearranges a little bit better, that when the time comes for the TSA to make a decision, what will we spend money on next, that all the technology and all the pieces for that tunnels of technology and checkpoint of the future will be there. So we think it is realistic. It is science fact, not science fiction, Mr. Chairman.

Chairman LIEBERMAN. Is there a lot of work going on in the private sector to develop these new technologies? This is a very significant global market, so I would think that people would be investing in it. Are they?

Mr. DUNLAP. Absolutely. We know from our experience with the manufacturers that all these advance technologies are currently under study. But the problem that we have right now globally is that every regulator has different technology standards. So something certified in the United States might not be accepted in the European Community.

Chairman LIEBERMAN. Right.

Mr. DUNLAP. It may not be accepted in Australia. So there is a good effort, and I would like to pay a lot of credit to TSA for working with like-minded countries to come up with the global standards. So if we have global standards of detection, that will accelerate and incentivize the manufacturers to invest in the technologies that we need. And then also, I think, having a common vision, what does the future look like, that can also incentivize dollars to be directed into a more predictable vision and a more compact vision of what we need to have in our airports.

Chairman LIEBERMAN. I appreciate that.

Mr. Barclay, let me ask you this question. As you know, TSA's Pre-Check pilot program has led to a separate line for trusted travelers. At this point, the line is managed by either Delta or Amer-

[1] The slide referenced by Mr. Dunlap appears in the Appendix on page 1284.

ican Airlines. Do you think this format will be successful if it expands to incorporate more passengers and airlines or should TSA be looking for another administrative means to expedite the screening of people?

Mr. BARCLAY. You have totally different facilities in each of the 450 airports, so airports have been concerned about continuing to have the ability to manage queues and lines. If you have been through Denver, they have a great big hall and the airport actually needs to manage those queues and lines because of the nature of the facilities. And that is going to be true at other airports, particularly as passenger levels grow. So we are going to need to have a partnership to figure it out as to how do we make a lane available. Our members strongly support the idea of Pre-Check. We are going to do our best with facilities, but there is going to be queue management and airports are going to have to be central to that.

Mr. DOW. Mr. Chairman, if I can add one comment——

Chairman LIEBERMAN. Go right ahead, Mr. Dow.

Mr. DOW [continuing]. I believe that just having an airline frequency program is not enough. Through the registered traveler programs that are out there, the data, the criminal records, all that, we can build a much broader base, and that is what we are saying must be done. We need to get a lot of travelers, folks like us that are trusted and able to get out of the system, because if you have a long line, that is what produces the problem. When you are trying to push people through during the peak times, that is when you have problems. So if you eliminate that, you have a much better chance of finding that needle in the haystack.

Chairman LIEBERMAN. Good point. Thanks. My time is up. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Dunlap, I am very intrigued by your proposal for the security screening based on risk and I do think that we need to move toward a more risk-based system and TSA is doing that, to Administrator Pistole's credit. I am, however, somewhat worried about the proposal and it is for this reason. If there is anything we know about al-Qaeda, it is that its members have demonstrated extraordinary patience over the years. So I am wondering, if we move to this system, what would prevent an al-Qaeda operative, perhaps someone like the Times Square would-be bomber, who was an American citizen, from traveling a lot, registering for the known traveler program, passing the background check, which he would have from everything we know, and just biding his time. And then, if he is only going through a lane that X-rays his carry-on bag and has him go through a metal detector, he could be lining his arms and legs with PETN, which would not show up.

And that is my worry. We know the patience. I mean, think of the number of years that elapsed between the first attack on the World Trade Center and the second. And we know the careful planning. So what is your response to that?

Mr. DUNLAP. Senator, we are acutely aware of the patience of our adversary and that is why we believe that, regardless of the concept, every passenger needs to be screened. They need to be screened for explosives. They need to be screened for weapons, as well.

So we establish a fairly high baseline within our concept to make sure that no one gets a free pass. Everyone is going to get screened.

You know, one of the interesting things about the proposal, whether you look at the lanes or you look at the tunnels, all of that incorporates processes that have been demonstrated to work already. So we have a known traveler lane. We have the Pre-Check plan that the TSA is piloting right now, which is an analog. We have Global Entry, which is an analog, and you can go through SENTRI and NEXUS programs, as well. So there is a demonstrated history that those type of programs work.

On the other hand, if you take a look at the high-security lane, that occurs in every airport in the world right now. In the U.S., you may see a glass booth, and within that glass booth, you will have a passenger getting swabbed down or have some other extraordinary security measure being taken to them. So our concept, it may look a little bit far forward, but that is what happens when you try to integrate things that are happening today in one place.

But certainly, we do not want anybody to get a free pass and we do not want anybody to walk through not getting screened. Everybody needs that when they get on an airplane.

Senator COLLINS. But although the known traveler gets screened, assuming I am reading your passport correctly, the baggage is screened through the X-ray machine and the passenger goes through a metal detector, but there would not be the kind of screening that is done with an AIT or an ATR, where you would see non-metallic explosives concealed on the body. Is that correct?

Mr. DUNLAP. Well, if you look at our concept over the next 7 years, it is to, in fact, develop walk-through explosive screening, walk-through imaging, so that can be done without a person having to spend 45 seconds of their time with their hands in a position like this getting screened and then going through the resolution process.

If you take a look at what we are proposing in 2 to 3 years, we are just talking about taking existing equipment, reordering it, and making it a little bit more efficient, because in the end, the efficiencies to be gained are by not having shout-outs in the airport checkpoint saying, take this bag, take this passenger and move them aside, because that slows down the lane.

So I think—and I confidently believe in this—is that we can establish a high enough baseline to ensure security, but also to do something, and that is to take the level of detection that we have right now, whatever that number is that the Committee has, and we can raise it even higher because we can direct our screening resources on those people that we know less about, least about, or those who appear on watch lists or another type of security list that the TSA has.

Mr. DOW. Senator Collins, if I could add one point——

Senator COLLINS. Yes, Mr. Dow.

Mr. DOW. One of the things that all security people tell us that deters this long-range planning is randomness, and when you have a randomness in the system, which Administrator Pistole adds, that enables us to thwart that in a very big way. So we are exploring, again, being able to go through this and having randomness, but when you have the random trusted traveler go through, just

make sure you are able to get them through that secondary and third screening very efficiently. So the randomness is very critical.

Senator COLLINS. Thank you.

Mr. Barclay, my last question is for you. Earlier this year, Administrator Pistole decided not to approve an expansion of the Screening Partnership Program, which allows private screeners to operate at 16 airports. What is your assessment of that decision?

Mr. BARCLAY. Well, our members support a viable and voluntary SPP program, so we would like to see revisiting that decision revisited. Most of the airports are not in the program. It is only 16 out of 450. There are a few others interested. But having it out there as an option is something that our members support.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins. Senator Moran.

OPENING STATEMENT OF SENATOR MORAN

Senator MORAN. Mr. Chairman, thank you.

Mr. Dow, you indicated that peak times is when there are problems. I just wanted you to tell me what the problems are. Are we talking about that it is more likely that someone who is a security risk will make it through security, or are the problems more related to the traveling public?

Mr. DOW. No, the problem actually is both. One, when you have an unpredictable system, you take the efficiency and the productivity of the American workforce away because you have to go through DCA an hour and a half in advance. But if you knew it would take 15 minutes, you would get there 40 minutes in advance.

But what happens during the peak time periods is the crowds get big, and you can see the urgency among the TSA sciences of how do we handle the crowd and move the lines. So if you are a bad person, you probably would want to go during one of those peak times. So we are saying, let us not have those large lines and create the incentive to try and get people through fast because it just does not work. Let us get an efficient system at all hours.

Senator MORAN. Thank you.

Mr. Dunlap, are there countries that we need to have concerns about the standards when passengers are screened and security procedures occur that are traveling around the globe, but particularly to the United States? How uniform are the standards by which the travelers are having to comply?

Mr. DUNLAP. Well, let me start with what I think is a very positive story that needs to be discussed. Globally, the level of security across the board has been increased immeasurably because of the investments of organizations such as the International Civil Aviation Organization and their efforts to raise aviation standards. But individually, countries have looked at the United States, have looked at other regulators, and have increased their own levels. So in terms of are we much safer globally than what we were immediately after 9/11? Unequivocally, yes, Senator.

And what I would say is if there are countries that are of worry, the best source of who they are and who their names would be would be with the intelligence community, and we trust that the men and women of the TSA have identified those countries and

have put in place procedures to deal with those additional threats that they might have. I would not be the intelligence specialist that would be able to name those countries.

Senator MORAN. Thank you, Mr. Dunlap.

And Mr. Barclay, I want to follow up on Chairman Lieberman's question that he raised with you about American and Delta, and I think your answer was, airports would like to have a lot of authority on those decisions, how we manage that program. You all have worked out the public-private partnership in regard to airport employees and their passage through security. Has that worked well, and is that what you were referring to when you were answering Senator Lieberman's question?

Mr. BARCLAY. No. They are really separate, but related to the extent that airports are experienced and do know how to do employee vetting. They would like to be sponsors of local Pre-Check programs so that Dulles Airport could have a program where in addition to the airline signing up people through frequent flyer programs, the airports could have an opportunity to have passengers show up, do the vetting necessary, and help people get enrolled who are not part of the frequent flyer programs. So airports have experience in how to get that information into TSA and we have eager members. After 9/11, you may remember that there was a privately-run registered traveler program that was sponsored by airports, and over 20 airports signed up for that and enrolled over a quarter of a million people. So airports would like to be part of Pre-Check.

The item that you mentioned on the clearinghouse is one that before 9/11, only about 10 percent of employees had to get criminal history record checks from the FBI and it was a nightmare. It was taking over 50 days to get a background check through the process because they were going through OPM. OPM was not set up to deal with entities outside of the Federal Government. They were losing accounting records.

Pre-9/11, we had research that the Bankers Association was doing criminal history record checks for banking employees. They had a clearinghouse to make those checks work smoothly for their industry.

That is what we set up in cooperation with FAA at the time and the airports. We have since vetted eight million backgrounds. It has not cost the Federal Government a penny, compared to the TWIC program, which has cost hundreds of millions and has vetted two million backgrounds. We have reduced that 50 days to minutes, which is what is important to an industry that is 24/7, needs to get employees vetted and out on the front lines as quickly as possible, to do that in a safe fashion. And it has really been a model of a public-private partnership that has worked very well.

The reason that AAAE got involved in that originally was that FAA ran security back then and Jane Garvey, who was the Administrator, selected us to do that because it was a co-op model. The customers of the clearinghouse are also the owners of the clearinghouse. Airport executives run the clearinghouse, make the decisions about its charges and operations, and they are also the customers on the other end. So that was the reason that we got into that program to begin with.

Senator MORAN. And that program has worked well?

Mr. BARCLAY. Very well.

Senator MORAN. And TSA is satisfied?

Mr. BARCLAY. They are, and they have moved in the last year to introduce competition so airports will have a choice of other vendors that can also provide those clearinghouse services, and we want to compliment TSA because they have moved on that carefully to make sure you did not undo a program that was working while you introduced more competition to it. So aviation workers, unlike truckers or port authority workers, who only have one program to go through and it is federally controlled, aviation workers are going to continue to have a variety, three options to go through, and they are in a program that costs about a third for the employee of what it costs a Haz-Mat trucker to get their vet done or a port worker to get their vet done. So it is a very efficient system and one that we would like to see TSA certainly continue.

Senator MORAN. Thank you, Mr. Barclay. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Moran.

Senator Landrieu, good morning. Thanks for being here.

OPENING STATEMENT OF SENATOR LANDRIEU

Senator LANDRIEU. Good morning. Thank you all. I think this is a very important hearing and I just wanted to highlight for the Committee's attention five items that are in the Homeland Security appropriations bill that will help expedite some of these initiatives.

We added in the Senate bill, Mr. Chairman, $10 million for TSA to begin to implement the trusted traveler program. It is in the Senate bill, not, unfortunately, in the House bill. A requirement for TSA to improve its response to passenger complaints, along with GAO review of existing procedures, is in the Senate bill, not in the House bill. Report language directing TSA to improve training to address passengers with physical or mental disabilities like autism, is not in the House bill but in the Senate bill. Eleven million dollars above the 2011 level to add 175 new Behavior Detection Officers, again, it is in the Senate bill, not the House bill. And there is a requirement that the fiscal year 2013 budget request documents resource allocation on the basis of risk, which is very important.

There may be others, but this is just a short list that I had my staff put together because the authorization, which happens in this Committee, is extremely important, but if it is not funded, it does not get done. And so I want to just thank Mr. Dow and Mr. Dunlap particularly for the input that your organizations have given us both in this Committee and in our appropriations process. I believe that your associations can really help us lead the way to the future, where we can have a very secure system but also a system that is much less intrusive than the one we have now so we can reduce the inconvenience and the frustration that is associated with traveling today.

And just for the record, Mr. Chairman, a 2010 survey by Consensus Research concluded that American travelers would take two to three additional flights each year if the hassles of security screening were eliminated. That would translate into an additional

$85 billion in consumer spending and 900,000 jobs created in the United States.

So this is an area of interest to us all from a variety of perspectives. It is for security and the safety of our Nation to prevent important attacks. But for the State that I represent that is in large measure dependent on the traveling public—we are an international destination, and we, like many communities, rely on those international travelers to sustain our economy—it is just imperative that we quickly develop the checkpoint of the future.

So I want to thank you all and I look forward to working with you.

My first question is on checked baggage, because I intend, Mr. Chairman and Ranking Member Collins, to file a bill to require the airlines, for every ticket purchased to allow one checked bag for free. If the airlines want to write it into their ticket costs, that is fine. But this is pushing so many bags into, as you all testified, carry-on luggage.

I understand that the cost, and if my staff will find this document, when Secretary Napolitano testified before our Committee, she testified that their internal study indicated that it cost TSA about $260 million more because of the baggage, Mr. Chairman, not being checked and being carried on. Is that your understanding? Do you have independent data? I will start with you, Mr. Dunlap and Mr. Dow.

Mr. DUNLAP. Well, Senator, that is certainly a very interesting question. What we do is we look at global trends. If you take a look globally at what is happening to checkpoints, the fact that they are slowing down, the fact that you are getting passengers more inconvenienced, that is happening regardless of whether or not the local business model there includes some sort of a la carte pricing, which is always being blamed for driving more bags into the checkpoints.

If you take a look at what is happening over time, IATA as far back as August 2005 sounded the alarm that our checkpoints were slowing down. So as you recall, in 2005, a la carte pricing or any kind of other pricing models that were discussed, they really did not exist in any major business models at all.

And then I think the last thing that you need to consider is what has been happening at security checkpoints over the last several years. Shoes have been coming off. Computers have been coming out. Liquids are being set aside. And now you have the body scanners where passengers have to take absolutely everything out of their pockets.

So I think, in all deference to the DHS report, I think that there are many other factors that are responsible for what is happening at the checkpoints rather than whatever or not the passenger puts the bag in the cabin or puts the bag into the belly of the aircraft.

Senator LANDRIEU. Mr. Dow.

Mr. DOW. Yes, Senator. You made two very important points. One was on the checked bags. Our research says that if people knew they could check a bag, if it was included in the price of their ticket, two-thirds would do so, and your point is right. You cannot dictate pricing to an airline, but we certainly can dictate that they should include that in the price of an airline ticket and it would help.

The second point you made, I thought was outstanding, is on customer service. TSA has to measure not only security, but customer satisfaction and efficiency, not on an average but at peak times, and have those measurements so we can look at them and know that we are satisfying the customers while improving security. So we agree.

Senator LANDRIEU. And Mr. Chairman, I really am very focused on this issue because I think it is increasing the public's anxiety and dissatisfaction with government generally. But Mr. Chairman, and I know it is not the purview of this Committee but rather the Commerce Committee, but if we do not do something, the airlines are going to sell a ticket to a flyer and you are not going to get a seat, you are going to stand on the airplane and then have to pay extra for the cushion, and I have about had it, OK? You do not get anything to eat. You get virtually nothing to drink. At least they give you water and a Coke or a 7-Up. Everything else costs.

So I think the American people deserve, when they purchase a ticket from an airline, they get one bag that they can check and a carry-on item in that ticket price and they absolutely get a seat and a glass of water. I mean, that should be the minimum Federal requirement, and I am going to push very hard to see that it gets done.

But in addition, let me just ask one final question to the airlines. Mr. Barclay, I flew in from Israel last week and got to the Newark Airport and was unable to use my cell phone from the time I exited the plane until I got, I guess, outside the building. Is that a rule of each individual airport or is that a TSA rule or where did that rule come from and are you aware of it?

Mr. BARCLAY. I will check on that and get back to you with the folks at Newark Airport. I presume it was just a cell usage problem that they——

Senator LANDRIEU. No, absolutely not. It was a restriction.

Mr. BARCLAY. Oh, you were told you could not——

Senator LANDRIEU. No one could use a cell phone from the time they got off the plane until they got their luggage through Customs and then out into the daylight, which, to me, when you are trying to manage business travel, the first thing people want to do when they have been traveling 13 hours on an international flight is check in with the office, see what they missed, etc. I wish, Mr. Dow and Mr. Dunlap, you would look at this. I do not know what the security requirement is for not being able to use cell phones. And, by the way, Mr. Chairman, we waited an hour and 10 minutes for our luggage after a 13-hour flight. And so the airports are going to be hearing from me about this baggage handling issue, as well, because it is very disappointing.

So as much as we can make the travel experience safe and convenient, it has to do with both the way people board their flight and the way they de-plane, and the exit portion is getting worse, just as the entrance portion is, so we have a long way to go.

I know I have exceeded my time. I thank you, Mr. Chairman.

Mr. BARCLAY. Senator, if I could just briefly, I am told that is a CBP rule that you are not allowed to use cell phones in the arrival area. So you could go back to them on that.

Chairman LIEBERMAN. We will take that up. I was going to tell you that if we are on the same flight together, I will give you my seat. I will not make you stand.

Mr. BARCLAY. You are going to stand?

Chairman LIEBERMAN. Yes. [Laughter.]

Senator LANDRIEU. You can stand up and hold on to the lavatory——

Chairman LIEBERMAN. Yes, and the cushion.

Mr. DOW. Senator Landrieu, I want to also thank you and the Appropriations Committee for what you are doing to help improve the visa process, because it starts when people start planning to come here, and the work you are putting forward there is going to make a huge difference in our economy. Thank you.

Chairman LIEBERMAN. Thanks, Senator Landrieu. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. To our witnesses, thanks so much for joining us today.

Senators Lieberman, Collins, Brown, and myself have a press conference in about 5 minutes on the U.S. Postal Service, so I am going to be very brief. In fact, I am going to pose a couple of questions and ask you to respond to them for the record.

The first question, Mr. Dunlap, is for you. I was intrigued by your discussion and images of the checkpoint of the future. The concept seems simple enough, and that is risk-based screening driven by information that we already collect from passengers, the use of advance screening technology, and separate lanes for different types of passengers. This kind of checkpoint, I think, could save travelers countless hours and ultimately increase the travel industry and our local economies.

Given the financial challenges that we face as a Nation, what would the checkpoint of the future likely cost taxpayers and are there programs and technologies in place right now that can be seamlessly integrated into your vision? That is a question for the record.

And maybe one more question for the record. This would be for all of our witnesses. In your testimonies, you discussed how the current one-size-fits-all screening process at America's airports does not meet the needs of our traveling public, and I think you also noted that we need to move to a system that detects dangerous people instead of dangerous things. And as you know, this Committee has continually challenged government officials to work smarter with Federal dollars and to find efficiencies in our government programs without compromising security. Our credo is how to get better results for either less money or the same amount of money without sacrificing security.

To this end, I understand that TSA has delivered a pilot to help expedite the flow of trusted travelers—you have had some discussion of that here today—but there is still much room for growth and improvement. Could you all discuss on the record for me the challenges that TSA faces as it looks to expand that pilot and how industry can help find solutions to these issues?

And I will have one more question, and I am not going to mention it today, but will submit another question or two for the record, as well, and if you could respond to those promptly, I would be most grateful. Thank you, sir.

Chairman LIEBERMAN. Senator Carper, I appreciate that very much.

I thank Mr. Dow, Mr. Dunlap, and Mr. Barclay. Your testimony has been very helpful.

We have come a long way. I mean, we are in a new age, and it is no fun, but as we have all said, the enemy is out there. The enemy is persistent and they continue to be attracted to air travel as a way to attack us and hurt us. We are trying very hard to protect the American people when they travel because the worst thing of all for airline business would be obviously if people felt unsafe.

But I think, increasingly, under Administrator Pistole, we are both trying to leverage new technologies but also move into, on top of the basics, a more risk-based approach, and that is exactly what I think all three of you are asking.

Your statements are in the record in full. We are going to keep the record of this hearing open for another 15 days for any additional questions or statements on either side of the bench here.

But I thank you very much for what you do every day and for the thought and effort that you put into your testimony this morning.

With that, the hearing is adjourned.

[Whereupon, at 11:30 a.m., the Committee was adjourned.]

APPENDIX

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"Ten Years After 9/11: A Report From the 9/11 Commission"
Homeland Security and Governmental Affairs Committee
March 30, 2011

Good morning and welcome to this first in a series of hearings where we will examine the many counter-terrorism changes enacted since the attacks of 9-11 with an eye towards building on what has worked and fixing what hasn't.

Today's hearing will be a general overview. In future hearings we will examine progress on specific challenges and security gaps exposed by the 9-11 attacks, including intelligence reform, aviation security, terrorist travel and emergency communications.

The attacks of 9-11-01 took place almost a decade ago but its memories are still so searing.

The nation watched on television as the mighty twin towers of the World Trade Center collapsed into a pile of smoking rubble, taking thousands of innocent lives with them.

American Airlines Flight 77 smashed into the Pentagon and set it ablaze.

And in the fields near Shanksville, Pennsylvania, we saw the smoldering crash site of United Flight 93, whose brave passengers fought to retake the plane from the terrorists who had targeted Washington, DC – saving hundreds if not thousands of lives by sacrificing their own.

In all, nearly 3,000 people died on what started out as a beautiful blue autumn morning.

But even as we mourned, we began to ask what went wrong and ultimately created the 9-11 Commission – legislation Sen. McCain and I sponsored – to investigate the flaws in our security and make recommendations to protect our nation against the terrorist enemy.

The Commission and its staff reviewed 2.5 million pages of documents, interviewed 1,200 individuals in 12 countries – including every relevant senior official of both the Clinton and George W. Bush Administrations – and held 19 days of public hearings across the country with 160 witnesses testifying.

The Commission's recommendations were sweeping, recommending both immediate actions we needed to take to defend our nation against further attack along with long-term actions we could take to blunt the terrorists' message and dry up their recruitment.

In response to the Commission's recommendations, this Committee authored and Congress enacted the Intelligence Reform and Terrorism Prevention Act of 2004 that created the Director of National Intelligence (DNI), whose job was to bring unity and coordination to the efforts of our nation's 16 separate intelligence agencies, and made the sharing of crucial intelligence at all levels of government the new standard operating procedure.

It also created the National Counterterrorism Center as the focal point for information-sharing and analysis of counterterrorism intelligence.

That Act was the most sweeping intelligence reform legislation since the creation of the CIA more than half a century before.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00375 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT
67123.001

This Committee was deeply involved in drafting these and other pieces of counter-terrorism legislation to implement the Commission's recommendations and further strengthen our security against terrorism.

But a lot of the hard work in identifying, recommending and then lobbying for specific reforms was done by the two men sitting in front of us this morning – Governor Tom Kean and Congressman Lee Hamilton, the chairman and vice chairman of the 9-11 Commission and now co-chairmen of its successor, the Bipartisan Policy Center's National Security Preparedness Group.

Welcome, gentlemen. And thank you again not only for your hard work and dedication to public service, but for providing our nation with a compelling reminder of what we can accomplish when we put aside party labels and work together for the national good.

I look forward to hearing your perspective on our nation's counterterrorism defenses, which I regard as a roadmap for future hearings and legislation this Committee should take up.

We're going to cover a lot of ground today, but there are three items of particular interest I would like to highlight.

One is your recommendation that we set aside the "so-called" D Block of the broadband spectrum for public safety departments – legislation Sen. McCain and I sponsored last year and will reintroduce in the near future.

Setting this broadband spectrum aside would allow us to build a robust, resilient and secure nationwide network for emergency communications that first responders could use to send video, maps and other large data transmissions over their mobile devices.

Police chiefs, fire chiefs, sheriffs and emergency managers across the nation overwhelmingly agree this is needed for them to save lives and protect property, and we should get that done in this Congress.

I was also pleased to see you are addressing cybersecurity in your newest recommendations. We have been working closely with Sen. Reid to develop a cybersecurity bill the Senate will consider this year.

"Cybercriminals" and "cyberspies" look at the Internet and see electronic pipelines that lead directly into everything from our personal bank accounts to government and industrial secrets.

And we have to prepare for the very real possibility of "cyber-war" and "cyber-terror" – the possibility, for example, that an adversary could take down our electrical grid or financial infrastructure from across the ocean with just a series of keystrokes.

Another question I'd like to explore in more detail with our witnesses relates to the powers of the Director of National Intelligence. I believe it is essential to have a strong Director of National Intelligence who can marshal the full capabilities of the Intelligence Community, and I am encouraged by some of the recent changes that the current director, Gen. Jim Clapper, has made toward further integration.

But I have been concerned for some time about bureaucratic resistance from the 16 intelligence agencies ostensibly under the control of the DNI and what that means for effective and efficient intelligence gathering and sharing. I see you both have the same concerns and I'd be interested in your specific recommendations.

Let me sum up as follows:

Since the 9-11 reforms, we have had many successes in our battles with the terrorists.

We've also had many close calls – like the shoe bomber and the Christmas Day bomber.

And we've also had some outright failures, like Maj. Nidal Hasan who radicalized right under the noses of the FBI and the Department of Defense and then murdered 13 people at Fort Hood.

We must continue to learn from our successes and our failures so we are not just constantly reacting to the last attack or attempted attack, but are taking the fight to our enemies.

I look forward to hearing our witnesses' recommendations and then working with them on future legislation.

We are also joined this morning by family members of three of the those 9-11 victims who went on to become leading advocates for the creation of the 9-11 Commission and the implementation of its recommendations.

They are Mary Fetchet, whose son Brad died at the World Trade Center; Carie Lemack, whose mother Judy was killed on American Airlines Flight 11 that crashed into the World Trade Center, and Abraham Scott, whose wife Janice was killed in the Pentagon.

Your work helped get the 9-11 reforms through Congress and I believe I can speak for the entire Committee when I thank you for your work.

67123.002

Statement of
Senator Susan M. Collins

"Ten Years After 9/11: A Report From the 9/11 Commission Chairmen"

March 30, 2011

This year, we will commemorate the worst attack ever on the United States. In doing so, we must ask ourselves, "Are we safer?" Or, are we just safer from the tactics the terrorists already have tried?

Is our intelligence community better at fitting together these complex puzzle pieces? Or have we just been lucky? Are we anticipating the next threat, such as a cyber attack or the use of poisons, or are we just looking backwards, reacting to previous plots?

Undoubtedly, compared to where we were on 9-10-2001, we have greatly improved the framework for information sharing among our intelligence and law enforcement agencies. But sometimes it has been an inept bombmaker or a faulty fuse that has spared American lives.

Once again, the two extraordinary leaders of the landmark 9-11 Commission, Lee Hamilton and Tom Kean, are appearing before our Committee as we evaluate our progress. In September of last year, their "Assessing the Terrorist Threat" report warned of an increasingly wide range of U.S.-based militants who do not fit any particular ethnic, economic, educational or social profile.

The American melting pot, the report said, "has not provided a firewall against the radicalization and recruitment of American citizens and residents, though it has arguably lulled us into a sense of complacency that homegrown terrorism couldn't happen in the United States."

This report correctly called 2009 a watershed year in U.S.-based terrorist plots, with 43 American citizens or residents aligned with violent Islamist extremists charged or convicted of terrorist crimes that year alone.

This Committee first sounded the alarm about home-based terrorism five years ago and has held 15 hearings on the topic. We found that individuals within the United States, in both our prison system and our communities, are being inspired by al-Qaeda's violent ideology to plan and execute attacks, often acting as "lone wolves" without direct orders from al-Qaeda.

67123.003

The Intelligence Reform and Terrorism Prevention Act of 2004, which Senator Lieberman and I authored, did much to improve the management and performance of our intelligence, homeland security, and law enforcement agencies. This most sweeping reform of our nation's intelligence community since just after World War II would not have happened without the leadership of our witnesses and the advocacy of the families of the victims. That increased collaboration and information sharing have helped our nation prevent numerous attacks.

There have been untold successes. In many cases, the intelligence community and law enforcement have quietly connected the dots and thwarted plots. In other cases, alert citizens reported suspicious behavior to authorities.

Challenges still remain, however. We continue to see troubling examples of a pre-September 11th, stove-piped mindset from some of our intelligence and law enforcement officers. For example, as documented in our Committee's recent report on the Fort Hood attack, the Army and the FBI collectively had more than enough information to have detected Major Hasan's radicalization to violent Islamist extremism, but they failed to act on the many red flags signaling that he had become a potential threat.

Major Hasan and others seem to find motivation and ideas online. Technology is transforming our culture, our economy, and our world in many beneficial ways. Yet, we must also be aware that terrorists seek to exploit the Internet's potential as well. We have witnessed recently that the Internet can serve as a platform for extremist propaganda on the one hand and peaceful revolution on the other.

Other Commission recommendations have not yet come to fruition. In particular, we must make more progress in enhancing first responder communications.

Gaps also remain at our borders and in our cargo inspection system. As the news today indicates, the potential to plant an explosive somewhere in the millions of pieces of air cargo shipped around the world daily is a real vulnerability.

It is also troubling that the Border Patrol does not have the ability to detect illegal activity across approximately three-quarters of the northern border. DHS must continue to work toward a balance that opens the border to our friends, while closing it to those who would do us harm.

Nonetheless, there have been real accomplishments—the biometric system for screening foreign nationals seeking to enter the United States, the creation of a consolidated terrorist watch list, and the dedicated DHS and state and local law enforcement employees deserve recognition.

67123.004

Even in these areas of progress, improvements are needed. Biometric screening should be expanded to include foreign nationals *leaving* the U.S. Screening technology must be improved to keep up with changing threats and to ensure that the safest possible screening equipment is deployed.

I hope this year we can expand protection against lawsuits for citizens who report suspicious behavior indicating potential terrorist activity. We also must pass legislation to ensure the key U.S. intelligence officials are consulted following a foreign terrorist's detention in the United States.

Finally, I continue to have deep concerns that this Administration refuses to acknowledge that violent Islamist extremism is the ideology that fuels such attacks. The Administration should have an overarching national strategy to counter this growing threat.

Ten years ago, nearly 3,000 lives were lost. We cannot become complacent or let down our guard when every single intelligence briefing that I've ever attended always warns that the enemy remains determined to attack our country.

Bipartisan Policy Center
Governor Tom Kean and Congressman Lee Hamilton
Testimony before the Senate Committee on Homeland Security and Governmental Affairs
March 30, 2011

Introduction

Mr. Chairman, Madam Ranking Member, members of the Committee: We are pleased to have the opportunity to appear before you today. This committee has been at the center of defending the country from the terrorist threat we face. We are deeply grateful to you for your sustained support of the 9/11 Commission's recommendations and leadership in reforming our national security institutions. Over the last decade, you have done much to ensure we are taking the difficult steps necessary to confront this determined enemy and protect Americans, our allies, and people throughout the world.

Today, we are appearing in our capacity as co-chairmen of the Bipartisan Policy Center's National Security Preparedness Group (NSPG), a successor to the 9/11 Commission. Drawing on a strong roster of national security professionals, the NSPG works as an independent, bipartisan group to monitor the implementation of the 9/11 Commission's recommendations and address other emerging national security issues.

NSPG includes the following membership:

Governor Thomas H. Kean, Former Governor of New Jersey; Chairman of the 9/11 Commission; and Co-Chair of the National Security Preparedness Group;
The Honorable Lee H. Hamilton, Former Congressman from Indiana; Vice-Chair of the 9/11 Commission; and Co-Chair of the National Security Preparedness Group;
The Honorable E. Spencer Abraham, Former U.S. Secretary of Energy and U.S. Senator from Michigan, The Abraham Group;
Mr. Peter Bergen, CNN National Security Analyst and Author, Schwartz Senior Fellow at the New America Foundation;
Dr. Stephen Flynn, President, Center for National Policy;
Dr. John Gannon, BAE Systems, former CIA Deputy Director for Intelligence, Chairman of the National Intelligence Council, and U.S.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00380 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.006

House Homeland Security Staff Director;
The Honorable Dan Glickman, former Secretary of Agriculture and U.S. Congressman;
Dr. Bruce Hoffman, Georgetown University terrorism specialist;
The Honorable Dave McCurdy, Former Congressman from Oklahoma and Chairman of the U.S. House Intelligence Committee, President of the Alliance of Automobile Manufacturers;
The Honorable Edwin Meese III, Former U.S. Attorney General, Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation;
The Honorable Tom Ridge, Former Governor of Pennsylvania and U.S. Secretary of Homeland Security, Senior Advisor at Deloitte Global LLP, Ridge Global;
The Honorable Frances Townsend, Former Homeland Security Advisor and former Deputy National Security Advisor for Combating Terrorism;
The Honorable Richard L. Thornburgh, former U.S. Attorney General, Of Counsel at K&L Gates; and
The Honorable Jim Turner, Former Congressman from Texas and Ranking Member of the U.S. House Homeland Security Committee, Arnold and Porter, LLP;

In recent months, our group has sponsored the following events:

- BPC Domestic Intelligence Conference featuring FBI Director Mueller and DNI Director Clapper-October 2010.
- Bridge-Builder Breakfast: Addressing America's Intelligence Challenges in a Bipartisan Way with House Intelligence Committee Chairman Rogers and Congressman Ruppersberger-March 2011.
- Press conference marking the release of the Bipartisan Policy Center's National Security Preparedness Group report, *Assessing the Terrorist Threat*-September 2010.

We believe the depth of this group's experience on national security issues can be of assistance to you and the executive branch and we look forward to continuing to work with you.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00381 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.007

Overview as We Approach the 10th Anniversary of the 9/11 Attacks

Now, nearly ten years after the tragic 9/11 attacks, and seven years since *The 9/11 Commission Report*, is an appropriate time to take stock of where we are in national security reform.

Effect of the 9/11 Attacks

The terrorist attacks of September 11, 2001 had a profoundly dramatic impact on government, the private sector, and our daily lives. The suddenness of the attacks on American soil and the loss of so many lives, made us feel vulnerable in our homes and caused us to question whether our government was properly organized to protect us from this lethal threat. The economic damage resulting from the attacks was severe. In short order, we shifted from a "peace dividend" at the end of the Cold War to the expenditure of massive amounts of taxpayer dollars on new security measures.

The consequences of the attacks for the private sector have been striking. More than 80% of our nation's critical infrastructure is owned by the private sector, and protecting it from terrorist operations has become an urgent priority. Working together, the government and private sector have improved their information sharing and thus our security posture.

Businesses in all sectors have adapted to this new reality. They have focused on how best to protect personnel and our food and water supplies; prepared continuity plans in preparation for possible disruptions; and altered how buildings are constructed, adopting innovative safety features. U.S. importers, working with the Department of Homeland Security, have pioneered new ways to ensure the integrity of shipping containers that bring goods into the country. The insurance industry's risk analysis has evolved to reflect new realities. These necessary innovations have increased the costs of doing business. Future innovations responding to the evolving threat may raise costs higher.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00382 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.008

The Government's Response

Over the past ten years, our government's response to the challenge of transnational terrorism has been equally dramatic. We have created major new institutions. The Department of Homeland Security itself amounted to a massive reconfiguration of government. As one indication of the scale of change to government, DHS now has a workforce of 230,000 people and an annual budget of $56.3 billion.

The Department of Defense and the Intelligence Community have also adapted. The military created a Cyber Command to respond to the increasingly alarming cyber threat. In 2004, with the leadership of Senators Collins and Lieberman, Congress created the Office of the Director of National Intelligence and the National Counterterrorism Center to ensure unity of effort in the Intelligence Community. There has been a dramatic increase in the intelligence budget. Some 263 organizations have been stood up or redesigned to assist in the effort. Across the national security community, a flexible and resilient workforce has been trained and is focused on protecting the American people.

Many of the 9/11 Commission's recommendations have been accepted and implemented, in whole or in part. Information sharing within the federal government, and among federal, state, local, and tribal authorities, and with allies, while not perfect, has been considerably improved since 9/11. The level of cooperation among all levels of government is higher than ever. State and local officials have a far greater understanding not only of the threat and how to respond to it, but also, their communities and those who may be at risk of radicalization.

The CIA, FBI, and the broader intelligence community have implemented significant reforms. As a result, in the years since the attacks, many plots have been disrupted and many terrorist operatives brought to justice.

Despite this considerable progress, some major 9/11 Commission recommendations remain unfulfilled. These require urgent attention because the threat from al Qaeda, related terrorist groups, and individual adherents to violent Islamist extremism persists.

The Threat Today

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00383 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.009

Smaller But More Varied Attacks

Al Qaeda and related terrorist groups continue to pose a serious threat to the United States. While much of al Qaeda's leadership has been removed, al Qaeda Central's top leaders, Osama bin Laden and Ayman al Zawahiri, are still at large. Although a devastating 9/11-type attack is less likely, the threat is more complex and diverse than at any time in the last decade. Al Qaeda and its allies continue to have the intent and the reach to kill dozens, or even hundreds of Americans in a single attack. There is a high risk of attacks, but they will likely be smaller.

The danger of al Qaeda comes not only from its core in Pakistan, but through its cooperation with other like-minded groups. Al Qaeda's influence is on the rise in South Asia and continues to extend into failing or failed states such as Yemen and Somalia.

Several factors, however, are working against al Qaeda and allied groups: the ramped-up campaign of drone attacks in Pakistan; Pakistani actions against some militants based on their territory; increasingly hostile attitudes toward al Qaeda and allied groups in the Muslim world in general; and the fact that some militant allies have now also turned against al Qaeda.

A key development in recent years is the increasingly prominent role and number of U.S. citizens and residents in the leadership of al Qaeda and aligned groups. Another development is the increasing diversification of the types of U.S.-based jihadist militants. Some are individuals inspired to engage in attacks on their own, while others have been actively recruited by overseas terrorist groups. Indeed these would-be jihadists do not fit any particular ethnic, economic, educational, or social profile. The operations they mount, or attempt, range from shootings, to car bombs, to suicide attacks to in-flight bombings of passenger aircraft.

In assessing terrorist threats to the American homeland, senior U.S. counterterrorism officials now call attention to al Qaeda's strategy of 'diversification'—mounting attacks involving a wide variety of perpetrators of different national and ethnic backgrounds. This strategy seeks to defeat any attempt to "profile" actual and would-be perpetrators.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00384 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.010

Radicalization

We have seen a pattern of increasing terrorist recruitment of American citizens. In 2009, there were two actual terrorist attacks on our soil. The Fort Hood shooting, claimed the lives of 13 people, and a U.S. military recruiter was killed in Little Rock, Arkansas. Indeed, many counterterrorism experts consider 2010 the "year of the homegrown terrorist." Last year, 10 Muslim-Americans plotted against domestic targets, and 5 actually carried out their plots. Today, we know that Muslim-American youth are being recruited in Somali communities in Minneapolis and Portland, Oregon, in some respects moving the front lines to the interior of our country.

Moreover, we know that individuals in the U.S. are engaging in "self-radicalization," Which is an alarming development. This process is often influenced by blogs and other online content advocating violent Islamist extremism. While there are methods to monitor some of this activity, it is simply impossible to know the inner thinking of every at-risk person. Thus, self-radicalization poses a grave threat in the U.S. Our group issued a report last Fall on this issue and will follow up this Spring with a set of recommendations for dealing with this important and sensitive problem.

New Threats

Our enemy continues to probe our vulnerabilities and design innovative ways to attack us. Such innovation is best exemplified by the discovery in October 2010 of explosives packed in toner cartridges, addressed to synagogues in Chicago, and shipped on Fed Ex and UPS cargo flights from Yemen. This plot constituted an assault on our international transportation and commerce delivery systems. Although it failed, terrorists will not abandon efforts to develop new ways to inflict great harm on us.

The Cyber Threat

Successive DNIs have warned that the cyber threat to critical infrastructure systems –to electrical, financial, water, energy, food supply, military, and telecommunications networks-- is grave. Earlier this month, senior DHS officials described a "nightmare scenario" of a terrorist group hacking into U.S. computer systems and disrupting our electric grid, shutting down power to large swathes of the country, perhaps for as long as several weeks. As the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00385 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.011

current crisis in Japan demonstrates, disruption of power grids and basic infrastructure can have devastating effects on society.

This is not science fiction. It is possible to take down cyber systems and trigger cascading side effects. Defending the U.S. against such attacks must be an urgent priority.

Status of the 9/11 Commission Recommendations

Emergency Preparedness and Response

Unity of Command

The 9/11 attacks demonstrated that even the most robust emergency response capabilities can be overwhelmed if an attack is large enough. Teamwork, collaboration, and cooperation at an incident site are critical to a successful response. We therefore recommended that emergency response agencies nationwide should adopt the Incident Command System (ICS); an essential element of this is that there be a unified command with one person in charge of directing the efforts of multiple agencies.

DHS incorporated ICS and the National Response Framework into the National Incident Management System (NIMS). NIMS provides nationwide guidance to clarify the roles of federal, state and local governments, NGOs, and the private sector in protecting against, responding to, and recovering from disasters. It has trained first responders throughout the country in the operation of NIMS.

NIMS was implemented during last year's Gulf oil spill. Its goal was to provide a unified, coordinated response under the leadership of DHS, with the Coast Guard as lead agency and BP as the responsible party. It divided the response into four main categories of effort: command, planning, operations and logistics. Each team was able to grow rapidly as more people arrived to respond to the spill. Management of the disaster was not without flaws, but in general it was an improvement over the often-fragmented approaches taken in response to previous disasters.

While the government has made some progress, our recommendation is still a long way from being fully implemented. Our discussions with community

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00386 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.012

leaders and first responders indicate that many metropolitan areas, with multiple agencies that would be involved in responding to a disaster, still have not solved the problem of unified command structure.

Radio Spectrum

The inability of first responders to communicate with each other was a critical failure on 9/11. Incompatible and inadequate communications led to needless loss of life. To remedy this failure, the Commission recommended legislation to provide for the expedited and increased assignment of radio spectrum for public safety purposes.

To date, this recommendation languishes. We find this unacceptable, because quite literally lives are at stake. The political fight has been over whether to allocate spectrum directly to public safety or auction it off to wireless bidders who would then be required to pay for a nationwide public safety communications network.

Initially, some advances were made when 10 MHZ of radio spectrum were allocated to public safety. The overwhelming majority of our nation's police chiefs and first responders, however, support the allocation of an additional 10 MHz of radio spectrum—the "D block"—to the existing dedicated public safety spectrum. Public safety agencies would be able to use the D block spectrum to build a nationwide interoperable broadband spectrum, allowing diverse agencies to communicate with each other, and supporting mission critical voice, video, text, and other data transmissions.

In his State of the Union address, President Obama called for allocating the D block spectrum to public safety. He also supports allocating $7 billion in federal funding to support a build-out of the network to ensure it reaches cash-strapped localities, especially rural communities.

We support the immediate allocation of the D-block spectrum to public safety. We must not approach these urgent matters at a leisurely pace. We don't know when the next attack or disaster will strike. Further delay is intolerable. We urge the Congress to act.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00387 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.013

Transportation Security

In the field of transportation security, a number of 9/11 Commission objectives have been advanced over the past two years. Airline passenger pre-screening and full implementation of Secure Flight fulfill our recommendation that TSA take over from the airlines the administration of the "no fly" and "automatic selectee" lists.

We are not satisfied, however, with the implementation of other recommendations. Additional funding has led to a major increase in the deployment at airports around the country of advanced screening equipment used in checkpoint explosives detection and in-line checked bag screening. Unfortunately, explosives detection technology lacks reliability. Airport body scanning machines are also not effective at detecting weapons, such as explosives, hidden within the body. Our conclusion is that despite ten years of working on the problem, the system still falls short in critical ways with respect to detection.

The Department of Homeland Security has improved international sharing of flight information substantially. The U.S. and the European Union now share information about passengers as soon as tickets are purchased, rather than after the plane has taken off, as was the case only a few years ago. Enhanced international cooperation should produce major gains in both air and maritime cargo security.

On the other hand, we still struggle to set priorities, define roles and implement a robust budget for transportation security. The GAO continues to identify serious holes in virtually every security layer.

Border Security

Since 9/11 and the creation of the Department of Homeland Security, a critical goal of our border security apparatus has been to prevent terrorists from entering the United States.

Border security remains a top national security priority, because there is an indisputable nexus between terrorist operations and terrorist travel. Foreign-born terrorists have continued to exploit our border vulnerabilities to gain access to the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00388 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.014

Terrorist Travel Intelligence

The 9/11 Commission recommended that the "United States . . . combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility." Every time terrorists travel they make themselves vulnerable to detection and interdiction.

While our government has made improvements, worrisome vulnerabilities remain in the system. Several attempted attacks over the past two years were perpetrated by terrorists who could have been detected by the U.S. immigration system. Examples include Christmas Day bomber Umar Farouk Abdulmutallab, who used a valid U.S. visa to board Northwest flight 253 in Amsterdam; Hosam Smadi, who plotted to blow up a Dallas office building after overstaying his visa; and Faisal Shahzad, who naturalized just over a year before attempting to detonate a massive car bomb in Times Square.

The U.S. government has the legal authority and infrastructure to secure against terrorist travel in a manner it did not prior to 9/11. Yet recent events suggest that further improvements can be made. In particular, a more streamlined terrorist watchlisting capability and improved information sharing between intelligence and immigration authorities should be priorities.

Biometric Entry-Exit Screening System

One area of great progress is the deployment of the biometric entry system known as US-VISIT. This system checks all individuals who arrive at U.S. borders, ensures they are who they say they are, and helps prevent known terrorists from entering the country. Data collected by US-VISIT are also used by homeland security, defense, law enforcement, and intelligence agencies for various important national security functions. US-VISIT has proven its value as a national security tool.

Yet despite the successful deployment of the entry component of US-VISIT, there still is no comprehensive exit system in place. As important as it is to know when foreign nationals arrive, it is also important to know when they leave. Full deployment of the biometric exit component of US-VISIT

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00389 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.015

should be a high priority. If law enforcement and intelligence officials had known for certain in August and September 2001 that 9/11 hijackers Nawaf al-Hazmi and Khalid al-Mihdhar remained in the U.S., the search for them might have taken on greater urgency.

Standardize Secure Identifications

Eighteen of the nineteen 9/11 hijackers obtained 30 state-issued IDs amongst them that enabled them to more easily board planes on the morning of 9/11. Due to the ease with which fraud was used to obtain legitimate IDs that helped the hijackers embed and assimilate in the U.S. for the purpose of carrying out a terrorist act, the 9/11 Commission recommended that "The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses."

The REAL ID Act established these standards by statute. In 2008, detailed regulations were issued setting standards and benchmarks for driver license issuance. While nearly one-third of the states have complied with the first tier of benchmarks, the deadlines for compliance have been pushed back twice to May 2011, and a recent announcement pushed back compliance again until January 2013. The delay in compliance creates vulnerabilities and makes us less safe. No further delay should be authorized, rather compliance should be accelerated.

In addition, there are still no minimum standards for birth certificates in place, as required by the Intelligence Reform and Terrorism Prevention Act of 2004. These standards are needed to close a back door that terrorists could use to obtain driver's licenses.

Intelligence Reform

Robust and well-organized intelligence capabilities are essential to protect the nation from the lethal terrorist threat we face today. We believed it was necessary to remove institutional blocks—legal, policy, and cultural barriers—between various agencies concerned with counterterrorism to forge a unity of effort across the intelligence community.

DNI

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00390 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.016

We recommended and Congress created the position of Director of National Intelligence. The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) made the DNI the principal intelligence advisor to the President, responsible for directing and coordinating the efforts of the 16 agencies of the intelligence community. In the six years since the creation of this post, the DNI has increased information-sharing, improved coordination among agencies, sharpened collection priorities, brought additional expertise into the analysis of intelligence, and further integrated the FBI into the overall intelligence effort. These are significant achievements.

At this time, however, it is not clear that the DNI is yet the driving force for Intelligence Community integration that we had envisioned. IRTPA left ambiguous the DNI's authority over budget and personnel. Such authority is critical to the success of the DNI. Secretary Gates and DNI Clapper reached a conceptual agreement last fall moving the intelligence budget under the DNI's purview. That will be of some help. But Congress needs to make clear the extent of the DNI's authority over both budget and personnel. The lines drawn should be bright.

It will then be the responsibility of the DNI to exercise that authority with discretion because it will bump up against authorities exercised by other powerful officials: Director of the CIA, DoD's Undersecretary of Defense for Intelligence, and the directors of the DoD intelligence agencies (DIA, NSA, NRO, and NGA). We are also concerned that there have been four DNIs in six years. Short tenures detract from the goal of building strong authority.

Strengthening the DNI's position would, we believe, advance the unity of intelligence effort that is needed. Legislation could fortify the office. Direct and repeated indication from the President that the DNI is the unequivocal leader of the intelligence community would also go far to strengthen his position and authority.

FBI

Since 9/11, the FBI has gone through wrenching change. A fundamental problem in responding to the growing threat posed by transnational terrorism before 9/11 was the FBI's culture. Traditionally, as a law enforcement organization, its managers and personnel have been steeped in that culture. In the years since the attacks, the FBI has shifted considerable resources and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00391 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.017

personnel from traditional criminal investigations to international counterterrorism and intelligence gathering. The changes have enabled it to make many arrests and disrupt many terrorist plots.

In 2005, we said that progress at the FBI was too slow. Since then, progress toward developing new functions and capacities has been significant but uneven. The change that has taken place has required real effort. The question now is: Have the reforms produced an integrated intelligence program within the FBI? This Committee's recent report on the Fort Hood shootings points to problems that still exist within the FBI. Specifically, It is not clear, for example, that analysts within the FBI are the drivers of intelligence that they ought to be at this time, or that they have achieved a status and importance within the FBI commensurate with the traditional power and management structure of the organization. Information the FBI and the military had on the alleged shooter, before the tragedy, was analyzed in terms of the threat of terrorism he posed but authorities failed to consider the counterintelligence implications it raised.

The failure of our government to prevent the Fort Hood tragedy also showed instances of poor communication among FBI Field Offices and between Field Offices and relevant offices within FBI headquarters. Restrictions on access to certain, sensitive FBI databases hindered some officials on detail to the FBI from fully understanding the potential threat posed by the perpetrator. These problems need to be addressed.

We are also concerned that the enormous effort to transform the FBI into an organization with an important focus on gathering and analyzing intelligence to prevent terrorist attacks may have diminished the Bureau's ability to vigorously enforce the criminal law and to investigate complex crimes.

The shift taking place within the FBI is a work in progress. More resources and more agents may well be part of the answer. Congress has a critical role to play. Through regular engagement and strong oversight it can help the FBI strike the right balance in its difficult transformation.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00392 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.018

CIA

The CIA is central to the fight on terrorism. It has been taking the fight to the enemy, relying on its dedicated officers and on cutting edge technology. To help CIA perform its vital role, we recommended that it rebuild its analytic capabilities; improve its human intelligence capabilities; develop a stronger language program; and recruit more diverse officers so they can blend more easily in foreign cities.

CIA has made some progress in breaking down the barriers between the spies who collect intelligence and the analysts who use the data for finished reports, going so far as to remove physical barriers in its operations center and other offices that had historically divided the two disciplines. Analysts and operations officers now train together beginning early in their careers. It has given specialists in 'open source' intelligence equal standing with spies and analysts in its key centers. It has stepped up use of its "intranet" in distributing reporting through secure networks maintained by the State and Defense Departments. It also makes greater use of alternative intelligence assessments produced by outside experts and has placed more analysts overseas. These are positive steps.

CIA and its oversight committees have been talking for many years about improving the Agency's human operations. Our sense is that there has been far more talk than action. To be fair, the fight against terrorism places huge demands on CIA. Over the past decade it has had to surge personnel to a number of war zones. While it has increased the numbers of its officers deployed overseas, added personnel strength and even greater funding do not necessarily result in better human operations. The simple fact is that it is very difficult to develop and recruit crucial sources, the ones with real access to decision making, in closed societies. Penetrating close-knit terrorist cells is also excruciatingly hard. But our national security demands that we make progress.

There are some larger, complex, and interlocking issues here. While we don't want to create permissive failure, it is important to recognize what CIA does is very difficult business. We want it to take risks in protecting the American people. Congress can help by depoliticizing oversight, removing the risk of political blame on those occasions when a necessary CIA operation fails, despite all reasonable planning, to achieve its aim, and results in negative blowback.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00393 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.019

In the 1990s our intelligence community had to deal with serious budget cuts. These had a negative effect on the strength of the CIA. Now, we are asking it to rebuild, during tough economic times. Former CIA leadership told the 9/11 Commission that it would take five years to rebuild the Agency. Building capabilities takes a long time. The workforce of CIA is young and a large percentage of its personnel have been added since the 9/11 attacks. Congress must provide the funding and support necessary to bring it to the level of excellence the threat we face requires.

CIA, despite having bolstered its language programs and recruited more people with specialized language skills, still does not have enough officers with fluency in the languages of greatest interest to our national security. The problem, however, does not just lie with CIA, or more broadly with the intelligence community. The fact is, our country deemphasizes language study. There are exceptions, of course, but in general our young people do not gain language proficiency in high school or college. To generate the pool of language proficient intelligence officers we need in the future, Congress and the Executive should develop, and implement through legislation, a strategy that will incentivize young people to learn and become fluent in difficult languages.

It is also imperative for CIA to recruit officers with diverse ethnic backgrounds. To operate effectively in the toughest and most challenging region of the world, to build relations with a diverse range of people, it helps to 'look like the world.' We continue to hear much about the difficulty of getting first-generation Americans through the security process. While we don't minimize security concerns, the intelligence community needs people with such backgrounds. This area needs to be rethought, so we can bring on board the people we need.

As the CIA is not transparent, it is difficult for us, or anyone outside the government, to assess with accuracy the status of implementation of recommended reforms. Because of the need to protect the CIA's sources and methods, only the intelligence oversight committees and a restricted circle of officials within the Executive Branch are briefed on the sensitive aspects of CIA's progress toward reform. We urge those officials to exercise vigorously their authority in order to help strengthen CIA and make it more effective. Among the important questions to be answered are: Has the quality of analysis improved? Are our policy makers receiving in a timely fashion the intelligence they need? How successful has the CIA been

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00394 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.020

in penetrating terrorist organizations? Do we have the capability to recruit the human sources we need? How do we measure success in both human operations and in analysis? Do we have sufficient numbers of clandestine officers in the regions that pose the greatest threat to our country?

Information Sharing

Legal, policy, and cultural barriers between agencies created serious impediments to information sharing before the 9/11 attacks. The 9/11 Commission made a number of specific recommendations to improve information sharing across our government. The formation of the National Counterterrorism Center was a major step toward improved information sharing.

We believe that information sharing has improved considerably in recent years. There are now 105 Joint Terrorism Task Forces throughout the nation, and 72 Fusion Centers in which federal, state, local, and tribal authorities investigate terrorism leads and share information. Since 2004, DHS has provided more than $340 million in funding to the Fusion Centers. Information sharing with the private sector has also become routine and is an important part of our defenses.

While the mechanisms are in place for better information sharing, the fact is that we missed opportunities to stop the Christmas Day bomber from boarding Northwest Flight 253, as well as opportunities to intervene before the Fort Hood shootings. Clearly there is much room for improvement. An enormous amount of intelligence information constantly pours into our national security system. Sifting through it, synthesizing it, making sense of it, and making sure it receives the necessary attention is a backbreaking challenge, one that requires attentive management and testing to determine where the flaws are and how to fix them.

The publication of sensitive government documents by organizations such as WikiLeaks has harmed our government's ability to conduct its affairs and has had serious consequences for our national security. It highlights the difficulty of striking a balance between the need to share information and at the same time preventing its unauthorized disclosure. Our government has the duty to prevent the unauthorized access to, and misuse or disclosure of, sensitive information. Appropriate sharing of information among authorized agencies and officials is essential to protecting the country from terrorist and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00395 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.021

other threats. Finding the right balance is not easy. Congress has a role to ensure that the Executive Branch is taking appropriate steps to address the problem.

Civil Liberties and Executive Power

The 9/11 Commission recommended the creation of a *Privacy and Civil Liberties Oversight Board* to look across the government at the actions we are taking to protect ourselves to ensure that privacy and liberty concerns are considered. Congress and the President enacted this recommendation. We commend the dedicated work of privacy officers in each of the respective agencies with national security responsibilities; they are doing their work with professionalism. In particular, assessments they have authored on the impact on civil liberties of policies, regulations, and directives issued by their respective departments have been strong.

But the government-wide board has been a disappointment. In fact, for more than two years it has been dormant. The Obama administration recently nominated two members for the Board but they have not yet been confirmed and the Board has not met.

If we were issuing grades, the implementation of this recommendation would receive a failing mark. We urge the Administration and Congress to address this failure in a speedy fashion. An array of security-related policies and programs present significant privacy and liberty concerns. A robust and visible Board can help reassure Americans that these programs are designed and executed with the preservation of our core values in mind. Board review can also give national security officials an extra degree of assurance that their efforts will not be perceived later as violating civil liberties.

Congressional and Administrative Reform

The 9/11 Commission said that oversight of intelligence was "dysfunctional." We strongly believed that "of all our recommendations, strengthening congressional oversight may be among the most difficult and important. So long as oversight is governed by current congressional rules and resolutions, we believe the American people will not get the security they want and need."

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00396 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.022

We recommended that Congress create a Joint Committee for intelligence or create House and Senate committees with combined authorizing and appropriating powers. We are disappointed that Congress has not fulfilled this recommendation. The basic issue is that agencies listen to the people who control their purse. But appropriations for CIA, for example, come under an already overburdened House Appropriations Subcommittee on Defense. The thrust of our recommendation is to ensure that there is credible, robust expert oversight of the intelligence community's funding and other activities. Our recommendation would ensure that the intelligence appropriations process was not an appendage to the massive defense budget. Last week, the Chairman of the HPSCI announced a decision to include three Members of the House Appropriations Committee to participate in House Intelligence Committee hearings and briefings. This is a positive step but there is more to do here.

Equally important, we recommended that Congress should create a single, principal point of oversight and review for homeland security. This, too, has not been done. The homeland security committees in the House and Senate do not have sufficient jurisdiction over important agencies within the Department of Homeland Security. Too many committees have concurrent and overlapping jurisdiction. Jurisdiction has been carved up to accommodate antiquated structures. This is a recipe for confusion. The upshot is that DHS receives conflicting guidance and Congress lacks one picture of how that enormous organization is functioning. Congress should be helping integrate the sprawling DHS; a fragmented oversight approach defeats that purpose.

We firmly reinforce what we said in our final report: That it is in our country's security interest that Congress make committee reform a priority.

Nonproliferation

The 9/11 Commission was deeply alarmed by Osama bin Laden's efforts to acquire nuclear weapons in the late 1990s. Our report concluded, "the greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons." We recommended that "Preventing the proliferation of these weapons warrants a maximum effort—by strengthening

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00397 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.023

counterproliferation efforts, expanding the Proliferation Security Initiative, and supporting the Cooperative Threat Reduction Program."

President George W. Bush said that "the biggest threat facing this country is weapons of mass destruction in the hands of a terrorist network." Sharing this assessment, President Obama said that "the prospect of nuclear terrorism is the most immediate and extreme threat to global security." While the likelihood of a terrorist mass-casualty attack may have diminished, the gravity of the harm were such an attack to take place would be enormous.

Currently, there are nearly 2000 tons of highly enriched uranium in dozens of countries around the world, enough to make 60,000 nuclear weapons. In light of this threat, in April 2010 President Obama hosted a Nuclear Security Summit of 47 nations. The Summit focused on the need to intercept trafficking in nuclear materials, enhance international cooperation, and improve the security of stockpiles. The Obama administration announced a new initiative to secure all vulnerable nuclear materials by 2013. In FY 2010 the administration asked for significant funding increases for all nonproliferation programs. It plans to spend $14.2 billion over the next five years to reduce the threat posed by nuclear and radiological materials.

Congress has not yet approved the FY 2011 budget. There are proposals to slash the National Nuclear Security Administration's budget for nonproliferation by as much as 22 percent. We must guard against any underfunding of this highest priority security need.

Develop Coalition Standards for Terrorist Detention

We recommended that the "United States should engage its friends to develop a common coalition approach toward the detention and humane treatment of captured terrorists" and that new principles might draw upon Common Article 3 of the Geneva Conventions.

Within days of his inauguration, President Obama signed a series of executive orders on the treatment of detainees and barring the CIA from using any interrogation methods not already authorized in the U.S. Army Field Manual. This ended CIA's authority to use harsh interrogation methods. The Administration is still grappling with how to close the Guantanamo prison facilities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00398 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.024

By bringing the U.S. into compliance with the Geneva Conventions and with international and customary law on the treatment of prisoners, the executive orders have substantially fulfilled our recommendation. Looking forward, however, we are concerned that the issue of how prisoners are to be treated has become so highly politicized.

This, we believe, is not good for the country or our standing in the world. Showing that bipartisan agreement is possible, and intending to reaffirm our values, the five Republicans and five Democrats on the Commission unanimously agreed on this recommendation. Together, we believed that our country's values require adherence to the rule of law and a commitment to human rights and humane treatment.

A lingering problem that two presidents have grappled with is how we reconcile the rule of law with keeping alleged terrorists in indefinite detention. For too long, the president and Congress have delayed resolving this difficult problem. In some cases we lack sufficient evidence against the detainees or the evidence that we have is problematic because of the way it was obtained. We regard as positive the Executive Order that requires periodic review of the status of prisoners at Guantanamo. Congress and the President must decide on a comprehensive approach that spells out clearly the rules of evidence and procedures and the forums in which they will be applied. Congress should anchor these decisions in a firm statutory basis.

Foreign Policy

As we meet here today, the Middle East and North Africa are in a state of upheaval. Exactly what will emerge from this unprecedented wave of protest sweeping the Arab world is unclear. While regime change or reform may move the region toward democracy, the ensuing instability could also be exploited by terrorists. Clearly, the United States would like to see governments emerge in the region that are inhospitable to terrorist organizations and that reject extremist ideologies. What can we do to enhance the likelihood of that outcome?

The 9/11 Commission explicitly addressed the critical role that U.S. foreign policy plays in counterterrorism, but did so with some modesty: Countries may share the common unifying thread of Islam, but each is different and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00399 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.025

has its own unique culture and traditions, requiring a country-by-country approach.

We said that tolerance, the rule of law, political and economic openness, and the extension of greater opportunities to women must come from within Muslim societies themselves. The United States must support such developments. Our relations with these countries must be based on our core values. We should seek democratic change and tolerance through pragmatic reform.

The protests and revolutions in the Middle East and North Africa region give us a degree of hope for reducing radicalization. Change and reform can reduce feelings of rage and despair, caused at least in part by political repression and economic stagnation. The call in the streets has been for democracy and political participation –not for bin Laden's version of jihad. It is worth noting, though, that the wave of protest does not yet seem to be touching Afghanistan or Pakistan—key countries identified in the 9/11 Commission's Final Report.

Public diplomacy (and nontraditional diplomacy more broadly) strikes us as essential in responding to the protests and change sweeping through the region. We should seek to foster reform, forestall gross human rights violations, and work closely with the international community, while avoiding putting the American imprimatur on the protests.

The key will be to engage pragmatically with the governments of the region to help them build stable institutions and provide immediate economic improvement to their people. We should support an agenda of opportunity for the Islamic world. People-to-people exchanges—between legislators, businesspeople, students, academics, civil servants, trade unions, lawyers, scientists, and other groups—could be very productive here. In The 9/11 Commission Report, we recommended that the United States "rebuild the scholarship, exchange, and library programs that reach out to young people and offer them knowledge and hope." A significant exchange program for emerging Middle East and North Africa democracies should be a relatively easy lift for Congress, and would be a tangible way of signaling U.S. friendship to the new democracies, on the basis of mutual respect and without seeming to meddle or to seek control.

The U.S. and European Union should also work together to use trade policy

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00400 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.026

to give a quick economic assist, in terms of market access, to the new democratic governments (once they emerge). Such an initiative would be much more effective if done in concert with the EU.

Reasons for the Success of the 9/11 Commission

We have reflected often on why the 9/11 Commission was successful. We think a number of reasons explain its success: First, because of the great damage and trauma the 9/11 attacks produced, the American public wanted action and had high expectations for measures and reforms that would improve the nation's security; importantly, the statutory mandate for the Commission was limited, precise, and clear—the Commission was authorized to investigate the facts and circumstances surrounding the attacks and to make recommendations to keep the country safe; the Commission had an extraordinary non-partisan staff, the members of which possessed deep expertise and conducted their work with thoroughness and professionalism; the Commissioners had deep experience in government and political credibility with different constituencies; the final report was unanimous and bipartisan; families of the victims of 9/11 provided solid and sophisticated support throughout the life of the Commission and in the years since; and following the Commission, the Commissioners and staff continued, to the present, to work closely with Congress and the executive branch to implement and monitor reform.

But the principal reason for the success of the Commission's work was that political leadership, including prominently the leaders of this Committee, embraced its findings and recommendations, pushed hard to enact them, and have continued to drive reform. Your support and leadership have been critically important in protecting the nation's security.

Conclusion

Significant progress has been made since 9/11, and our country is undoubtedly safer and more secure. Yet important 9/11 Commission recommendations remain to be implemented. Over the next two years there is heavy lifting to be done. To date, Congress has resisted reorganizing its own institutions. Streamlining congressional oversight of the Intelligence

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00401 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.027

Community and Department of Homeland Security would go far toward advancing unity of effort in the intelligence community and within DHS.

It is also time for a clear-eyed appraisal of how the Office of the DNI is functioning, as well as the state of reform in the FBI. We have concerns about each, and our goal should be to strengthen both. While our group brings together well-informed experts with deep experience in government and counterterrorism, we are at a disadvantage: We cannot conduct investigations; we cannot compel people to come forward and state candidly what is not working; and we cannot review classified documents. This Committee, and other committees, has that authority. The American people rely on you to continue asking the hard questions, as this Committee has done so effectively in the past.

Over the last 10 years, we have damaged our enemy, but the ideology of violent Islamist extremism is alive and attracting new adherents, including right here in our own country. Close cooperation with American Muslim communities is the key to preventing the domestic radicalization that has troubled some of our European allies. Positive outreach and efforts to foster mutual understanding are the best way to prevent radicalization and sustain collaborative relationships.

Our terrorist adversaries and the tactics and techniques they employ are evolving rapidly. We will see new attempts, and likely successful attacks. One of our major deficiencies before the 9/11 attacks was that our national security agencies were not changing at the accelerated rate required by a new and different kind of enemy. We must not make that mistake again.

The terrorist threat will be with us far into the future, demanding that we be ever vigilant. Our national security departments require strong leadership and attentive management at every level to ensure that all parts are working well together, that there is innovation and imagination. Our agencies and their dedicated workforces have gone through much change and we commend them for their achievements in protecting the American people. But there is a tendency toward inertia in all bureaucracies. Vigorous congressional oversight is imperative to ensure that they remain vigilant and continue to pursue needed reforms.

Our task is difficult. We must constantly assess our vulnerabilities and anticipate new lines of attack. We have done much, but there is much more to do.

Thank you for inviting us to testify, and for this Committee's longstanding leadership on these critical issues.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00402 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.028

JOSEPH I. LIEBERMAN, CONNECTICUT, CHAIRMAN

CARL LEVIN, MICHIGAN
DANIEL K. AKAKA, HAWAII
THOMAS R. CARPER, DELAWARE
MARK L. PRYOR, ARKANSAS
MARY L. LANDRIEU, LOUISIANA
CLAIRE McCASKILL, MISSOURI
JON TESTER, MONTANA
MARK BEGICH, ALASKA

SUSAN M. COLLINS, MAINE
TOM COBURN, OKLAHOMA
SCOTT P. BROWN, MASSACHUSETTS
JOHN McCAIN, ARIZONA
RON JOHNSON, WISCONSIN
JOHN ENSIGN, NEVADA
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY

MICHAEL L. ALEXANDER, STAFF DIRECTOR
NICHOLAS A. ROSSI, MINORITY STAFF DIRECTOR

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

April 8, 2011

The Honorable Barack Obama
The President of the United States
The White House
1600 Pennsylvania Avenue, NW
Washington DC, 20500

Dear Mr. President:

We are writing to express our deep concern about the lack of a functioning Privacy and Civil Liberties Oversight Board and to urge you to nominate a full slate of members for the Board as quickly as possible.

As you know, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) authorized a Privacy and Civil Liberties Oversight Board to ensure that efforts to combat terrorism do not encroach on vital freedoms. The Board was a recommendation of the 9-11 Commission, which recognized that new efforts to prevent and deter terrorism might impinge on critical privacy and liberty concerns. In the words of the Commission, "At this time of increased and consolidated government authority, there should be a board within the executive branch to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." The Commission's report went on to state, "Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

The original Board did begin this important oversight work. Congress subsequently concluded that its status, within the Executive Office of the President, did not allow it enough independence. In 2007, as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), Congress reconstituted the Board as an independent entity outside the White House, with a full-time chairman and enhanced authorities, including subpoena authority through the Attorney General.

Unfortunately, this effort to create a more robust Privacy and Civil Liberties Oversight Board has instead resulted in no board at all. Although the Board was meant to begin its work in 2008, the Bush Administration and your Administration have been slow to select nominees for the new five-member Board. Two nominees are now before the Senate Judiciary Committee, but even if they were immediately confirmed they would not have a quorum to conduct business. It is imperative that the Administration complete its nomination process so that Congress can then expeditiously fulfill its advice-and-consent role and allow the new Board to begin its critical mission.

The 9/11 Commission Chair Thomas Kean and Vice-Chair Lee Hamilton strongly reiterated the need for the new Board in testimony before the Homeland Security and Governmental Affairs Committee last week, and we agree. We have been strong supporters of the nation's expanded homeland security and counterterrorism capabilities but recognize that they present the potential for increased governmental

intrusions into individuals' lives and therefore bear careful monitoring. Noting the privacy and civil liberties concerns that the array of security-related policies and programs present, Kean and Hamilton stated that "a robust and visible Board can help reassure Americans that these programs are designed and executed with the preservation of our core values in mind." Kean also told the Committee that "nothing has frustrated me more" than the failure to create the Board the Commission envisioned. We share Chairman Kean's frustration. It is inexcusable that, more than three years after the new Board was meant to have begun its work, there is still no functional board at all. We ask that you give this matter your prompt attention and stand ready to work with your Administration to help the Board begin its work as soon as possible.

Sincerely,

Joseph I. Lieberman
Chairman

Susan M. Collins
Ranking Member

Daniel Akaka
Chairman
Subcommittee on Oversight of Government
Management, the Federal Workforce,
And The District of Columbia

Post-Hearing Questions for the Record
Submitted to Hon. Thomas H. Kean and Hon. Lee H. Hamilton
From Senator Daniel K. Akaka

"Ten Years After 9/11: A Report from the 9/11 Commission Chairmen"
March 30, 2011

1. After 9/11, the Intelligence Community (IC) addressed its workforce deficiencies in part by hiring a large number of contract employees. According to the Washington Post, contractors now make up close to 30 percent of the IC workforce. This raises a number of concerns, including the high cost of intelligence contractors relative to federal employees, potential conflicts of interest because of loyalty to shareholders rather than to the public interest, management and oversight challenges, and the potential for contractors to perform core government functions reserved for federal workers.

    a. What do you believe are the implications of our dependence on contractors in the IC?

    b. Do you believe the IC should reduce its reliance on contractors?

    c. How would you suggest that the federal government proceed in addressing the specific concerns outlined above?

Answer:

There are vital intelligence collection and analysis functions that can only be performed effectively by government employees. In some cases, however, contractors serve in these roles. This frequently occurs because the federal government was not able to recruit and train employees in sufficient time. In areas where the intelligence community (IC) is unduly reliant on contractors, the IC should take steps to improve its human intelligence capabilities.

As noted in our written testimony, the CIA in particular needs to continue to improve its human capital. In the 1990s, serious budget cuts had a negative effect on the strength of the CIA. We have asked it to rebuild during tough economic times, and building capabilities takes a long time. Congress should provide the funding and support necessary to bring it to the level of excellence justified by the threats we face.

The CIA should recruit officers with diverse ethnic backgrounds who can blend more easily into the populations of foreign cities. To operate effectively in the toughest and most challenging regions of the world, to build relations with a diverse range of people, it helps to "look like the world."

The human capital situation in the IC could be improved by empowering the Director of National Intelligence (DNI). The *Intelligence Reform and Terrorism Prevention Act* left ambiguous the DNI's authority over budget and personnel. Such authority is critical to the success of the DNI.

Congress needs to make clear the extent of the DNI's authority over both budget and personnel, which would allow the DNI to address concerns about overreliance on contractors. The lines drawn should be bright. Direct and repeated indication from the President that the DNI is the unequivocal leader of the intelligence community would also go far to strengthen his position and authority.

67123.031

2. Currently, the IC largely prevents the Government Accountability Office (GAO) from conducting reviews of IC programs, which limits Congress's ability to conduct oversight of IC activities. To address this, the Intelligence Authorization Act for Fiscal Year 2010 requires that the Office of the Director of National Intelligence (ODNI) develop a directive governing GAO's ability to review components of the IC. In response to my question for the record following a 2007 Committee hearing entitled "Ensuring Full Implementation of the 9/11 Commission Recommendation," Representative Hamilton stated that GAO should have the same authorities within the IC as it has in other agencies.

    a. Do you believe that allowing GAO to conduct reviews within the IC – particularly of management functions such as financial systems and workforce planning – would contribute to improved Congressional oversight of IC programs?

    b. How should GAO's ability to review IC programs differ, if at all, from GAO's ability to conduct reviews of non-intelligence federal programs?

    c. Do you believe that the ODNI directive should establish an IC-wide set of standards that each component must follow in interactions with GAO? To what degree should the ODNI directive allow each component of the IC discretion regarding its cooperation with GAO?

Answer:

The GAO should have the authority to audit and evaluate IC management functions, such as its financial systems, just as it does for non-IC federal government agencies. The GAO's review of IC functions, however, needs to be done with appropriate protections for classified information that generally do not apply to non-IC agency audits.
The Fiscal Year 2010 Intelligence Authorization Act required the Director of National Intelligence to issue a directive governing access of GAO to information in the possession of an element of the intelligence community. Pursuant to the statute, this directive must be written in consultation with the GAO. We hope that this consultation process resolves GAO access issues and minimizes differences between IC components in the access provided to GAO.

3. The 9/11 Commission noted the shortage of language proficient speakers in this country in its 2004 report. This is a long-term, complex problem – stemming in part as you note from lack of educational emphasis on language proficiency – within the IC and throughout government. The 9/11 Commission recommended developing and implementing a strategy to incentivize young people to become fluent in difficult languages.

    a. What key elements would you recommend including in this strategy?

    b. What additional steps would you recommend that the Executive Branch and Congress take to address current and future language needs?

Answer:

A government-wide approach must be taken to promote and incentivize proficiency in languages needed by our government and the private sector because no one agency has the resources or authorities to address the problem. A key element of a language strategy would be ensuring the promotion of difficult languages that are needed by the intelligence community. To fully understand the gaps in language skills of the intelligence community, the Office of the Director of National Intelligence should play a role in the strategy's development.

67123.032

Post-Hearing Questions for the Record
Submitted to Hon. Thomas H. Kean and Hon. Lee H. Hamilton
From Senator Claire McCaskill

"Ten Years After 9/11: A Report from the 9/11 Commission Chairmen"
March 30, 2011

1. As you know, we continue to focus extraordinary resources in Afghanistan where we have over 100,000 troops and are spending billions of dollars in security operations and development activities. While I remain committed to our efforts in Afghanistan, I am also compelled to ask the hard questions as our endeavors slog onward and as the nature of the threats against our homeland shift.
    a) In the current environment, from what location, if you had to pick one, is an attack against our homeland most likely to emanate / where do you feel the greatest threat to our national security exists?
    b) Where is Al Qaeda most active in the world today in your view and why?
    c) If you had to rank North Africa, Pakistan, Yemen and Afghanistan in order of where an attack is most likely to be organized and/or originate against the United States, how would you do so?

Answer:

Because of the diffuse nature al Qaeda and its affiliated groups, it is not possible to identify one country as the most likely source of a terrorist attack against the United States. While the death of Osama bin Laden was a blow to the core of al Qaeda, we cannot let our guard down. Al Qaeda and its affiliates are persistent and their associations and tactics are diverse. The threat emanates not just from al Qaeda's core in Pakistan, but from affiliates in other parts of South Asia and in failing or failed states such as Yemen and Somalia, and increasingly from homegrown terrorists.

For example, al Qaeda in the Arabian Peninsula (AQAP), which is part of the broader extremist movement and only has a loose connection to core al Qaeda's leadership, has become a highly menacing threat to the United States. This group was behind the attempted 2009 Christmas Day bombing of a passenger plane bound for Detroit. An American cleric now residing in Yemen, Anwar al-Awlaki, has a prominent role in AQAP.

Moreover, senior U.S. counterterrorism officials now call attention to al Qaeda's strategy of "diversification" – mounting attacks involving a wide variety of perpetrators of different national and ethnic backgrounds who do not fit any particular ethnic, economic, educational, or social profile. This strategy seeks to defeat any attempt to "profile" would-be terrorists based, among other factors, on their nationality.

67123.033

2. As you stated in your testimony, radicalization and homegrown terrorism are emerging as one of the most serious threats to this country now that al Qaeda cells abroad and here in the United States appear to be splintered and disorganized. While it is good news that we have been successful in fracturing some of al Qaeda's operations, thwarting attacks from these less organized and dispersed factions of Al Qaeda across the globe pose significant challenges.
   a) How do local law enforcement and intelligence communities work together to thwart the threat you have recognized?
   b) With all of the political uprisings occurring right now in the Middle East, and our recent involvement in the political movement in Libya, do you anticipate any repercussions here in the United States?

Answer:

a) Within the federal government, the formation of the National Counterterrorism Center, which integrates terrorism threat information, was a major step toward improved information sharing. The diverse threats from terrorists around the globe, however, mean that an enormous amount of intelligence information constantly pours into our national security systems. Improved management and a willingness to address flaws in the intelligence community (IC) are essential to ensuring that the IC effectively sifts through the information, synthesizes it, makes sure it receives the necessary attention, and passes it along to state and local law enforcement and the private sector when appropriate.

   Information sharing between the federal government and state and local officials has improved considerably in recent years. There are now 105 Joint Terrorism Task Forces throughout the nation, and 72 Fusion Centers in which federal, state, local, and tribal authorities investigate terrorism leads and share information. Since 2004, DHS has provided more than $340 million in funding to the Fusion Centers. Information sharing with the private sector through DHS's private sector coordinating councils also has become routine and is an important part of our defenses.

   At the federal, state, and local levels, we need to look to technology to help us better sort through massive amounts of information to ensure the right people are seeing it in time to make a difference. The technology we use must be state of the art, constantly upgraded to quickly put information together, and it must be properly placed so better analysis can occur instantaneously.

   While the mechanisms are in place for better information sharing, the fact is that the government missed opportunities to intervene before the Fort Hood shootings and to prevent the shooting of the Army recruiter in Little Rock, Arkansas. Clearly, there remains much room for improvement.

b) The Arab Spring may help to counter the violent extremist agenda. Where al Qaeda failed attempts to destabilize Arab governments, peaceful protesters have succeeded through their grassroots uprisings in achieving regime change and dramatic political reforms.

   But these revolutions are not without risks. If they falter and fail to build a new democratic world, groups aligned with al Qaeda could emerge again. The current instability in Libya and elsewhere could serve as a breeding ground for these groups. Their resurgence would be the greatest potential danger to the homeland from this overall significantly positive development.

67123.034

3. Since 9/11, the federal government has infused Homeland Security and intelligence agencies with billions of dollars. The issue of cost effectiveness is rarely addressed. During your testimony you stated that we "need a hard-headed person to make sure monies are being spent wisely."
    a) Can you explain what you meant by that statement?
    b) Do you think Congress is spending money for security and intelligence in a manner that makes the most sense? If you were still in Congress how would you allocate our "scarce resources"?

Answer:

The priority in the years after 9/11 for the nation's homeland security and intelligence agencies has been to increase their capabilities. This focus on expanded capability has not been matched by a focus on cost effectiveness. Attention to cost effectiveness, particularly in these difficult fiscal times, is long overdue.

To ensure that homeland security grant programs are cost effective, the 9/11 Commission recommended that grants be targeted to areas where there are the greatest risks. Despite a recent effort by the Department of Homeland Security (DHS) to prioritize its Urban Area Security Initiative grant program on the cities with the greatest risk, other homeland security grants are allocated so that each state receives a certain minimum amount. Federal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks and vulnerabilities that merit additional support.

In addition, the Government Accountability Office has identified several homeland security programs that would benefit from risk management approach to the deployment of resources, which seeks to maximize the security benefits from the use of scarce resources. Congress should ensure that DHS and other federal agencies implement the GAO's recommendations for better risk management.

67123.035

4. Another troubling issue that emerged from the 9/11 response was inadequate unity of command. On the national level and in response to the 9/11 Commission, Congress created the Director of National Intelligence (DNI) – an office designed to coordinate all intelligence related matter.
   a) Do you believe the DNI functions as originally envisioned?
   b) If not, why? Do you have any recommendations on how Congress can fix the problem?
   c) Do you believe DNI's authority is appropriately recognized at the federal level? Please explain.

Answer:

We recommended and Congress created the position of Director of National Intelligence. The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) made the DNI the principal intelligence advisor to the President, responsible for directing and coordinating the efforts of the 16 agencies of the intelligence community. In the six years since the creation of this post, the DNI has increased information-sharing, improved coordination among agencies, sharpened collection priorities, brought additional expertise into the analysis of intelligence, and further integrated the FBI into the overall intelligence effort. These are significant achievements.

At this time, however, it is not clear that the DNI is yet the driving force for Intelligence Community integration that we had envisioned. IRTPA left ambiguous the DNI's authority over budget and personnel. Such authority is critical to the success of the DNI. Secretary Gates and DNI Clapper reached a conceptual agreement last fall moving the intelligence budget under the DNI's purview. That will be of some help. But Congress needs to make clear the extent of the DNI's authority over both budget and personnel. The lines drawn should be bright.

It will then be the responsibility of the DNI to exercise that authority with discretion because it will bump up against authorities exercised by other powerful officials: the Director of the CIA, the Secretary of Defense, DoD's Undersecretary of Defense for Intelligence, and the directors of the DoD intelligence agencies (DIA, NSA, NRO, and NGA). We are also concerned that there have been four DNIs in six years. Short tenures detract from the goal of building strong authority.

Strengthening the DNI's position would, we believe, advance the unity of intelligence effort that is needed. Legislation could fortify the office. Direct and repeated indication from the President that the DNI is the unequivocal leader of the intelligence community would also go far to strengthen his position and authority.

67123.036

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"Ten Years After 9/11: Is Intelligence Reform Working?"
Homeland Security and Governmental Affairs Committee
May 12, 2011
As Prepared for Delivery

Good afternoon and welcome to this second in a series of hearings this Committee will hold to examine how well the national security reforms implemented in the wake of 9-11 are working and where improvement is needed.

We hold this particular hearing – "Ten Years After 9/11: Is Intelligence Reform Working?" – in the aftermath of a spectacularly successful collaboration between our intelligence and military agencies that resulted in locating and killing Osama bin Laden, the al Qaeda leader who presided over the 9-11 attacks on America.

This success required intense and focused cooperation among key intelligence agencies – the Central Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the Office of the Director of National Intelligence – and the Defense Department.

Each organization brought its distinct areas of expertise to bear on the clues that had been gathered about bin Laden's suspected hiding place. All this data was then pulled together to reach informed conclusions with a level of confidence that allowed President Obama to act decisively.

I don't believe this would have happened 10 years ago. In fact, the 9-11 Commission expressed its frustration that no one was in charge of our government's hunt for Osama bin Laden, even after he killed almost 3000 Americans on our own soil. That symbolized the dysfunction and disunity that contributed to 9/11 in the first place.

In response to the 9-11 Commission's criticisms, this Committee drafted and Congress passed the Intelligence Reform and Terrorism Act of 2004, the most sweeping intelligence reform since the creation of the Central Intelligence Agency more than 50 years ago.

Among its many improvements, the intelligence reform bill created a Director of National Intelligence – or DNI – to harness the efforts of our 16 intelligence agencies and offices under one yoke in order to make them work together towards the single goal of collecting and analyzing intelligence so we can better defend against the threats to our nation – especially the terrorist plots we know are being planned, rather than simply react after an attack.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

The 2004 Act also created the National Counterterrorism Center to ensure that there was a single place in the government that would assess terrorism threats using the full resources and knowledge of the intelligence community and the wider government.

So is the killing of bin Laden proof that the new system works and the spirit of collaboration prevails? I would say yes. But the hunt for bin Laden – a mass murderer the entire free world wanted jailed or dead – was clearly a unique case.

The President, the Secretary of State, the Secretary of Defense and the heads or our national security apparatus were directly involved in evaluating the evidence and drawing up plans to kill or capture bin Laden.

When the scrutiny is not at this level, the evidence about how improved the functioning of the Intelligence Community is is mixed.

There have been impressive successes. Perhaps the most impressive is Najibullah Zazi, who received training from al Qaeda and was arrested in September 2009 with the plans and chemicals needed for a bombing attack in New York City. The plot was foiled by cooperative work among our intelligence agencies and local and federal law enforcement.

But we have seen failures, like Farouk Abdulmutallab, the Christmas Day bomber, and Times Square bomber Faisal Shazad, who both slipped through our intelligence networks.

Most notably, this Committee's report on the attack at Fort Hood, Texas, by "lone wolf" terrorist Maj. Nidal Hasan, painfully detailed how this tragedy was preventable. Clues to Hasan's Islamist radicalization and the potential danger he posed were hiding in plain sight in front of the FBI and the Department of Defense, but they didn't share the information or ignored it.

We need to ensure that the shoulder to shoulder cooperation we saw in the hunt for bin Laden, who already attacked us, is being applied to all those lurking in the shadows planning fresh attacks, because the death of bin Laden does not mean the death of Al Qaeda or Islamist terrorism.

Core al Qaeda has been greatly weakened but is not yet vanquished. Al Qaeda affiliates still operate in the Arabian Peninsula, Somalia, Iraq, and the Sahel. All pose dangers to the American homeland and our allies everywhere.

And the threat of homegrown "lone wolf" terrorists like Hasan is growing.

Our revamped intelligence community must take on these challenges and more.

Since its creation, the DNI has also helped the intelligence community to focus its efforts on new priorities, such as Cybersecurity and led the effort to update the FISA law, which governs surveillance of U.S. citizens, making our intelligence agencies more effective in collecting information on terrorist organizations.

DNIs have also established a joint-duty personnel program that requires personnel of one intelligence agency to rotate to another as a condition for promotion – thus encouraging cooperation and creating trust where there had been rivalries.

67123.038

But, despite these great improvements, in this hearing we want to ask whether the DNI has all the authority it needs to truly be in charge of our sprawling intelligence community.

So today, I want to explore the DNI's authority over the intelligence budget and the hiring and firing of senior personnel, as well as other authorities in the 2004 legislation.

I want to understand if the DNI is now the leader of the intelligence community that we envisioned – and accountable for its performance. Or is the DNI primarily a manager who focuses on such functional matters as budgets, personnel, and technology while other officials handle the operations?

And if the DNI is not really in charge of the intelligence community, who is?

To answer these and other questions, we have before us today a stellar panel with vast expertise on intelligence issues. They are:

Former Congresswoman Jane Harman, who served as ranking member of the House Permanent Select Committee on Intelligence, where she worked closely with Senator Collins and me on the Intelligence Reform and Terrorism Prevention Act. She later chaired the House Homeland Security Committee's Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment;

General Michael V. Hayden, former director of the Central Intelligence Agency, former director of the National Security Agency, and former Prineipal Deputy Director of National Intelligence;

And John Gannon, former Assistant Director of Central Intelligence for Analysis and Production and one of our nation's premier experts on intelligenee analysis.

We thank you all for coming today and look forward to your thoughts about where we are and where we need to go to ensure our intelligence community consistently performs at the high level we saw demonstrated in the hunt for bin Laden.

67123.039

Statement of
Senator Susan M. Collins

"Ten Years After 9/11: Is Intelligence Reform Working?"

May 12, 2011

I would like to thank our distinguished panel for being here today. We have an impressive line-up indeed: former Representative Jane Harman, one of the authors of the Intelligence Reform and Terrorism Prevention Act. Representative Harman worked closely with Senator Lieberman and me in crafting the 2004 reforms; John Gannon who has had a stellar career in the Intelligence Community having served as the Deputy Director of Intelligence at the CIA and Chairman of the National Intelligence Council; and, Michael Hayden whose extraordinary service includes his tenure as the First Principal Deputy Director of National Intelligence and the Director of both the CIA and NSA.

Last week's welcome news that Osama bin Laden was killed demonstrates the kind of successful collaboration of intelligence and operations that we envisioned in reforming our capabilities and intelligence community in the wake of the attacks of 9-11-01.

This is a great victory for our intelligence efforts and a great blow to al Qaeda. But al Qaeda is not going away.

That is why it is time for Congress to examine and build on the successes that emanated from the Intelligence Reform and Terrorism Prevention Act, identify any shortcomings, and work to correct them.

Our 2004 law created the Director of National Intelligence and the National Counterterrorism Center to foster information sharing and collaboration among our security partners.

The DNI has made concrete progress integrating the 17 agencies and departments in the intelligence community. Let me give just two examples of how that integration is taking place:

In 2008, the DNI rolled out the innovative "A-Space," which is an intelligence analyst's Facebook. But instead of social networking, our intel experts are posting, sharing, and asking each other about topical issues. They can collaborate with colleagues across agencies and around the world, allowing them to share leads and resources more easily than ever.

67123.040

I also am pleased that the National Counterterrorism Center has created "pursuit teams" that map terrorist networks, track threats using information from across intelligence agencies to bridge the gaps between national and domestic intelligence, and put pieces of the intelligence puzzle together.

These are just two examples of innovative ways stovepipes have been broken. Given the influx of intelligence analysts who joined the IC after 9 - 11, I am hopeful that this new generation is less wedded to the silos of the past. I believe that the more senior managers also are embracing the increased collaboration and information sharing that have helped prevent numerous attacks during the past decade. The arrests of Najibullah Zazi and David Headly were just two of many cases where we have connected the dots.

On the other hand, this Committee concluded in our investigation on the Fort Hood shootings that the DoD and the FBI collectively had sufficient information to have detected Major Hasan's radicalization to violent Islamist extremism, but that they failed act effectively on the many red flags signaling that he had become a potential threat.

Almost 10 years since September 11 and seven years since our landmark legislation, we are safer but not yet safe. Our intelligence community is stronger and more effective than ever before, but plenty of turf battles remain.

To help address these and other deficiencies in the IC, the DNI must be the quarterback that the 9-11 Commission envisioned and we intended. In this Administration, however, there is the potential for the DNI to be trumped by unconfirmed czars, who are not accountable to Congress but enjoy extraordinary power and proximity to the President.

At our earlier oversight hearing, the leaders of the 9-11 Commission, Governor Kean and Congressman Hamilton, agreed that John Brennan is, in many respects, performing the role we envisioned for the DNI when we authored the legislation. That troubles me, not due to any doubts about Mr. Brennan's capabilities, but because that structure undermines the statutory role of the DNI.

We must ask whether changes to the law are required, or whether more fidelity to the 2004 law is the answer to realizing the potential of the DNI.

The successful operation against bin Laden opens the door to another challenge. How can we make the most of what is reported to be a treasure trove of information found at the compound? The agencies scrubbing and analyzing the data must work together and build a bridge between foreign leads and domestic leads. If the American intelligence community uses the data found to its fullest, more terrorists will be captured or thwarted, and Americans will be more secure.

67123.041

The Honorable Jane Harman
Testimony before the
Senate Homeland Security & Governmental Affairs Committee Hearing
"Ten Years After 9/11: Is Intelligence Reform Working?"
May 12, 2011

It is a pleasure to testify before dear friends and dedicated colleagues who serve on one of the most important and bipartisan committees in the Senate. I am passionate about the topic of this hearing: intelligence and intelligence reform were the focus of my 17 years (119 dog years) in the House. I didn't run an intelligence agency like one of the other witnesses today, but I did conduct careful oversight over the intelligence function for many years.

Although 24 heroic NAVY SEALS deserve our nation's gratitude for the capture and kill of the world's most wanted man, the information on which their mission was based derived, in most part, from the integration of people and "ints" achieved by the Intelligence Reform & Terrorism Prevention Act of 2004 (IRTPA).

We now have proof that IRTPA works – that, at its best, our Intelligence Community can achieve the "seamlessness" that its authors dreamed of.

In fact, my view is that if we had not passed IRTPA and had continued to operate the IC using the 1947 business model set out in the National Security Act, we would probably not have been able to thwart a number of plots, or take down OBL.

Let me address 3 issues:

1. Performance of the Director of National Intelligence (DNI),
2. Role of domestic intelligence agencies, and
3. Ongoing problems with Congressional oversight.

The Director of National Intelligence

The DNI continues to be a work in progress. Congress intended her/him to be a joint commander – far more than a coordinator. And the job clearly requires leadership skills.

IRTPA is not a perfect law but contains adequate authorities to give the DNI the necessary leverage. I often say that the function is 50% law and 50% leadership.

Congress intended the DNI to serve as principal intelligence advisor to the President. This has never happened. During the Bush administration, Vice President Cheney was the principal advisor. During the Obama administration, it has been John Brennan. In my view, neither President truly valued the DNI role nor has made an adequate effort to support the function.

67123.042

But the role is evolving and I am pleased with certain reforms undertaken and proposed:

1. Taking the National Intelligence Program out of the Defense Department budget, as DNI Clapper suggests, will make budgeting more efficient and promote accountability.
2. Right-sizing the staffing and reducing the use of outside contractors within the Office of the Director of National Intelligence is crucial. The authors of the legislation believed the old CIA Community Management Staff was adequate. The right DNI doesn't need a bureaucracy.
3. Working closely with the Secretary of Defense. It helps that Gates – and soon to be Panetta – were CIA Directors. This close cooperation was impossible in 2004 given Secretary Rumsfeld's implacable opposition to the law. That's why we were forced to include section 1018, which fortunately, has been "clarified" by E.O. 12333.
4. Reducing the number of Congressional reports. I agree with DNI Clapper. I know why they originate, but better to consolidate them and build trust. Eliminating unnecessary work will save money and keep focus on the mission.

Other challenges include:

1. Collection relies too heavily on classified information. The Arab Spring shows the importance of social media and we must adapt our methods.
2. The privacy and civil liberties function is anemic. I commend this Committee for its efforts to stand up a fully functioning Privacy & Civil Liberties Board, which is not currently operational. Without the Board, US government efforts to improve defenses against critical threats like cyber attack remain opaque and scary. The public doesn't understand why the National Security Agency is in the public sector cyber business, and the Department of Homeland Security (DHS) hasn't been able to explain its role adequately either. We need public buy-in if these programs are to be successful, since most information networks are private. In my view, this Board is an essential tool to vet cyber programs and in giving the public confidence about them.
3. Another priority for the Privacy & Civil Liberties Board is the domestic mission space, which needs greater clarity. The entire intelligence community must be more dynamic and responsive to homegrown threats so that we can provide law enforcement and the public with helpful warnings about suspicious activities. If we are tracking US persons, we must impose the protections of the Constitution and the Foreign Intelligence Surveillance Act Amendments to access information regarding American terror suspects.

The National Counterterrorism Center and the Department of Homeland Security Office of Intelligence & Analysis

Problems persist with vertical information sharing – a role of each of these agencies.

67123.043

President Bush established TTIC (Terrorist Threat Integration Center) outside DHS because he felt the new department was too slow to stand up I&A. TTIC was first headed by John Brennan, and became NCTC in 2004 (in the Intelligence Reform law). Current NCTC Director Mike Leiter is very able, and the ITACG (Inter-Agency Threat Assessment and Coordination Group), mandated by Congress and located at NCTC, helps prepare usable products for law enforcement.

I&A played a robust role in the Bush Administration when headed by CIA legend Charlie Allen. The role appears to have been downsized by the Obama Administration. The CT function at DHS is coordinated by Undersecretary Rand Beers, not by I&A.

The key to preventing or disrupting an attack in a US city is to share accurate and actionable information with first responders in real time. Otherwise, they won't know what to look for or what to do.

We continue to have a problem with overclassification of information. I commend this Committee and its able staff for helping to pass the Reducing Overclassification Bill last year. The law establishes procedures to promote information sharing with state, local, tribal, and private sector entities, and provides training and incentives to promote accurate classification of information by federal employees. Its goal is to reduce unwarranted secrecy. Now we need to implement it.

Beyond the problem of overclassification, I&A struggles to meet an enormous mandate. In order to prevent duplication, I suggest that the I&A role become more focused on borders and infrastructure since these are "value added" pieces of intelligence collected by DHS.

Finally, the quality and capability of local fusion centers is uneven. Many are fantastic and provide DHS and the Federal Bureau of Investigation with actionable information based on Suspicious Activity Reports and other tips (ie Zazi and Shahzad cases). Some are not. Clear guidance must be available for these centers to sift through mass amounts of information that may help thwart the next plot. DHS must continue to be vigilant about ensuring privacy protections at these centers and that a privacy officer is assigned to each center. This is another critical area where the Privacy and Civil Liberties Board could be incredibly useful.

Congressional Oversight

This Committee has far more jurisdiction than its House counterpart on which I served for 8 years, 4 of them when it was the Select Committee. But the 9/11 Commission recommendation to reorganize Congress has never been fully implemented.

I'm pessimistic that anyone in Congress will voluntarily give up jurisdiction. One idea which is unlikely to be accepted is to give the Intelligence Committees appropriations authority. (I bet a few appropriators in this room will oppose this.) Chairman Mike Rogers' initiative to allow 3 appropriators to participate in the work of the House Intelligence Committee is a good effort, but doesn't constitute adequate reorganization. We must do more.

Conclusion

There is no way to make the homeland 100% safe. What we can do is minimize risk. We need to reevaluate constantly the threats against the US and prioritize our investments – both financial and brain cells – to defend against them.

Finally, let me recognize the brave women and men of our intelligence community who put their lives on the line everyday for our country – often in austere places around the world, living apart from their families. They are the true heroes and the people who will benefit most from clear intelligence guidelines and authorities.

67123.044

Testimony of Michael V. Hayden
U.S. Senate Committee on Homeland Security and Governmental Affairs
May 12, 2011

Chairman Lieberman and Ranking Member Collins, thank you for inviting me to offer an assessment of the impact of the Intelligence Reform and Terrorism Prevention Act of 2004 on U.S. Intelligence Community reform, and to comment more specifically about the adequacy of the authorities which the 2004 Act conferred on the Director of National Intelligence.

My testimony today closely tracks the views I expressed in an article that I published in 2010 *World Affairs,* an international affairs journal. The views I expressed then remain unchanged.

The 2004 Act, the very direct result of your hard work and commitment, established the new position of DNI, who was given two principal tasks. The DNI was to serve as senior intelligence advisor to the President. He also was to enhance the Intelligence Community's coordination and integration.

It is the DNI's second task – that of enhancing the IC's coordination and integration – that I will focus on today. But before I do, I would like first to briefly review the historical context that led to this legislation being proposed and approved by Congress, and signed into law by President George W. Bush.

In 2004, Congress, as were we all, was frustrated by the IC's failure to prevent the 9/11 attacks and its faulty national intelligence estimate on Iraq's weapons of mass destruction. As a result, Congress felt it needed to act. Because it is difficult to legislate better analysis, more aggressive intelligence collection, or perfect covert action, Congress faced three more limited choices in reacting to these failures: it could move money, move people, or restructure organization charts and strengthen authorities.

Congress chose the last option – organizational restructuring and enhancing authorities. Its goal arguably was to recalibrate for the Intelligence Community the critical balance that any complex organization needs: the balance between freedom of action for the parts and the unity of effort for the whole. Too little autonomy for the parts leads to inaction, inflexibility, hesitation, and lost opportunities. Too little unity of effort means that individual excellence is not synchronized, harmonized, exploited, or leveraged.

In short, Congress was determined to strengthen the center of the Intelligence Community. In doing so, it relocated and renamed the center. The director of central intelligence, also known as the DCI, would become the director of national intelligence, referred to as the DNI, who would be no longer serving in the dual-hated role of both director of the Intelligence Community and the Central Intelligence Agency. Rather, the DNI's sole responsibility would be to direct the Intelligence Community. Indeed, the legislation directed that the DNI was not even to be allowed to have his offices at Langley, where the CIA has its headquarters.

I was very concerned in 2004 about the merits of reorganizing the Intelligence Community. I thought doing so would be a drain on time and energy, during a period when we were waging relentless and successful global war against al-Qaeda and providing, at that point, valuable and accurate analysis on post-invasion Iraq. I also disagreed with the notion that the former DCI was not especially strong. The DCI under whom I had spent significant time working while I was director of the National Security

67123.045

Agency, George Tenet, used to task me regularly. In fact, I believed that the strongest "glue" we that we had in terms of creating unity of effort and operational cohesion within the Intelligence Community was the DCI. He was head of the Community, while at the same time he headed up the operationally relevant agency within, the CIA.

But I also understood and believed even more strongly that the DCI's role of the head of CIA brought inherent limitations. It was difficult, if not impossible, for a single individual to effectively perform both as head of the community and CIA. The DCI would be challenged to make resource allocation tradeoffs between human and signals intelligence when he was the head of the agency responsible for human intelligence.

As a result, I was equally convinced that, if we were going to establish the new position of DNI separate from the CIA director, then we had to make sure that the legislation dealt the new office a very powerful hand – and that it did formally and specifically. Indeed, that is what I recall recommending to you both when we met in the summer of 2004.

Lt. Gen. James Clapper, then head of the National Geospatial Intelligence Agency and now DNI, and I warned the House Permanent Select Committee on Intelligence later that summer that a "feckless" DNI would actually make matters worse than not having a DNI. Lt. Gen. Clapper and I also met with then-Defense Secretary Rumsfeld and his team and made the case for the Defense Department supporting a strong DNI.

Our fears were realized when Congress inserted language into the reform bill stipulating that, in exercising any robust authorities that the two of you successfully inserted into the legislation elsewhere, such as budget control, the DNI could not abrogate the authorities of the cabinet officers of department in which elements of the Intelligence Community were located. Section 1018 of the bill represented an effort to protect the sectary of defense's prerogatives when it came to his critical combat support agencies: the National Security Agency, the National Geospatial Intelligence Agency, and the National Reconnaissance Office.

In the end, this section was modified so that it required the president to issue guidance on what the DNI could and could not do in order not to abrogate cabinet officers' authorities.

The Bush Administration attempted to issue such guidance by revising Executive Order 12333, the basic document through with the president organizes and controls the Intelligence Community. The order was badly in need of update, having been issued in 1981 by President Reagan and rarely modified since. As part of the revision process, an attempt was made to soften the affect of Sec. 1018 by including a presumption that the DNI's activities were not an abrogation of cabinet secretaries' authorities. After much effort, however, the final version of the executive order repeated that the DNI shall not abrogate the authorities of the various department heads.

Another factor that undermined efforts to strengthen the center of the Intelligence Community was the creation of the undersecretary of defense for intelligence – or USDI. The USDI was stood up a year before Congress had even begun to focus seriously on intelligence reform, and this new position foreshadowed the challenges that lay ahead in for those attempting to strengthen the Intelligence Community's center.

67123.046

In establishing the position of USDI Secretary Rumsfeld, who had been dissatisfied with the intelligence he had been receiving, placed an empowered Pentagon official between the national intelligence chief – then the DCI, now the DNI – and several his biggest collection entities, the National Security Agency and the National Geospatial Intelligence Agency. When Secretary Rumsfeld later delegated his "authority, direction and control" of the major Defense Department intelligence agencies to the USDI, he effected major reorganization and power shift in the IC. By the time Congress turned its full attention to intelligence reform in 2004, that critical shift was already locked in.

Whatever its merits, the concept of the USDI cuts across the grain of legislation designed to strengthen the "center," to give the leader of the national intelligence community more strength, and to give the DNI more say over the current operations and future direction of the entire intelligence community.

The relationship between the DNI and the CIA director is also critical. The 2004 law states that the DNI shall recommend to the President the candidate to be CIA director. However, in my experience this has only happened once – when DNI Negroponte recommended me to be the CIA director. Director Negroponte and I overlapped, with him as DNI and me as CIA director, for only six months. By all indications, DNI Blair played no role in the selection of Leon Panetta to be CIA director.

Even in the best of times, the relationship between the DNI and the CIA director is a challenging one. The 2004 law puts the DNI at the center of the Intelligence Community, but the CIA has pride of place and a culture that is very reluctant to admit otherwise. While CIA director, I would frequently say that since the CIA director and the DNI were on or near the same grid reference, the only way to prevent fratricide was to separate us at different altitudes. The DNI should work at the higher altitudes—set policy, give overall direction, manage conflict – whereas the DCIA should work the lower by coordinating, conducting, and operating. The CIA director must guarantee the DNI transparency; the DNI has to give the CIA director space to operate. This sounds simple, but the DNI under whom I served after DNI Negroponte's departure, Admiral Mike McConnell – we had known each other for years, were friends, and between us had nearly three quarters of a century of intelligence experience – and I still found that this relationship took a lot of effort.

The complexity of the law, competing conceptions of what it meant, and the sheer magnitude of the Intelligence Community's global mission and reach meant that success depended upon a series of intangibles: the DNI's political deftness, the DNI's closeness to the President, and the DNI's relationship to the CIA director.

DNI Blair did not know President Obama before being appointed as DNI. He made some well-intentioned moves that caused him to have to dig out of political holes. In addition, the Obama administration moved the DNI down the protocol list and seemed to have little interest in the Intelligence Community's inner workings.

DNI Blair and CIA Director Panetta became embroiled in a dispute concerning a DNI directive stating that the DNI could name his own representatives overseas. The issue had come up when I was CIA director, and I resisted advice to take this issue to the White House because I thought there was no way that the White House would fail to back the DNI on an issue of authority. But when the issue got to the White House in the Obama administration, the administration backed the CIA director. The DNI lost, and lost publicly.

After DNI Blair's departure, a news story clearly sourced to White House officials described Mr. Brennan as the President's "invaluable go-to person" on many intelligence questions. Simultaneously, the current Secretary of Defense, Robert Gates, suggested that the DNI position is closer to that of "a powerful congressional committee chair than it is to a CEO."

We are thus left where we began: a continuing effort to balance unity of effort with autonomy of action. This is never easy. I have said in other fora that the current structure is as good as any in giving us a chance to make it happen. But our experience does point out the limits of structure and the importance of personal relationships and other intangibles.

Opening Statement of
John C. Gannon
to the
US Senate Homeland Security and Government Affairs Committee
Hearing titled "Ten Years After 9/11: Is Intelligence Reform Working?"
Room SD-342, Dirksen Senate Office Building
12 May 2011, 2:30 p.m.

Mr. Chairman and Members of the Committee:

I retired from the Intelligence Community (IC) nearly 10 years ago, but have remained involved with it ever since. In my career, I held senior positions including CIA's Deputy Director of Intelligence, Assistant Director of Central Intelligence for Analysis and Production, and Chairman of the National Intelligence Council. After retirement, I worked in the White House Transition Planning organization for the Department of Homeland Security, heading the team for Information Analysis and Infrastructure Protection. I subsequently served for two years as the staff director of the House Select Committee on Homeland Security and briefly as the first staff director of the permanent Homeland Security committee.

Since government retirement, I have served voluntarily on various research committees and task forces supporting US intelligence agencies. I am currently a sector president of BAE Systems, which provides products and services to customers including the US defense and intelligence communities. From all these experiences, I have observed the performance of the IC in recent years with keen interest, though I clearly no longer qualify as an insider. My comments, therefore, should be seen as informed impressions rather than authoritative assessments, but hopefully they will be helpful in any case.

I will address the six questions provided by the Committee staff on 5 May:

1. ***Should the DNI be a coordinator, manager/integrator, or leader? What is the DNI's role currently?***

The Director of National Intelligence (DNI) should be seen as a leader with explicit responsibilities for clearly defined, selective oversight of IC performance, for the development and application of interagency program standards, and for the implementation of the National Intelligence Program. These responsibilities must be seen as legitimate by the IC leadership and workforce, which requires, in turn, that they be backed up by the Executive and Legislative branches. The actual role of the DNI today falls short of all this, despite the strong efforts of four capable incumbents since 2005 to fulfill IRTPA's intent. The DNI is a manager, coordinator, facilitator, and troubleshooter, not the leader of the Intelligence Community. The CIA Director appears to report to the DNI only on paper and leaders of the Executive Branch and Legislative Branch seem to consult with major agency heads in a crisis as much as with the DNI.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00422 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.048

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 states its intention to establish the position of DNI with three core responsibilities: (1) to serve as the head of the intelligence community; (2) to act as the principal adviser to the President, to the National Security Council, and to the Homeland Security Council for intelligence matters related to national security; and (3) to oversee and direct the implementation of the National Intelligence Program. This, in my view, implied a significant shift of power from multiple, heavily resourced agencies in an increasingly decentralized community to an historically weak center with minimal resources. What we have today is an ODNI that is considerably stronger and more effective than the former Community Management Staff but way short of IRTPA's model of a central authority.

IRTPA did not delineate any practical architecture for an incumbent to do this difficult job and it did not anticipate the extent to which leaders of the Executive and Legislative branches would continue to rely on the legacy intelligence agencies rather than the DNI for advice on priority intelligence matters. The DNI, with negligible top cover, has been left to fight for legitimacy among more powerful agencies, some of which resist existing DNI authorities, let alone invite new ones. And legitimacy is still the core issue.

More broadly, the legislation drafted in 2004 underestimated the impact of the irreversible movement of the IC over the past 20 years toward a distributed model of intelligence support that defies centralized leadership. Military leaders, diplomats, civilian agency heads and homeland intelligence customers all want real-time intelligence support dedicated to their missions and priorities. In my judgment, the legislation underestimated the extent to which the changing global threat environment and the resulting decentralizing pressures on the IC would strengthen individual agencies and frustrate any DNI's efforts to establish centralized authority. More than ever, globalization enables the delivery of real-time intelligence and close-in operational support anywhere in the world.

Finally, the IC's distributed services delivery model increasingly runs in parallel with a distributed leadership model that, in the nature of the intelligence business, will always be somewhat ragged at the edges — at least that's the way successive Presidents have managed it. From crisis to crisis, program to program and issue to issue, the DNI, the SECDEF, the CIA Director, or a key military commander may be in direct, sustained contact with the President and/or the National Security Council, and this is unlikely to change. And, in my view, this in itself would not necessarily undercut the broader authorities of a strong DNI.

The DNIs have instituted constructive programs to improve intelligence tradecraft, to integrate intelligence collection and analysis, to increase information sharing, and to promote interagency collaboration. They also have used their "bully pulpit" to good effect. But the position has not achieved a level of legitimacy among IC agencies to give confidence to an incumbent DNI that he can fully exercise existing authorities, let alone any new ones, in a manner that the agencies will accept and that both the Administration and the Congress will support. The DNI is still burdened by the longstanding IC principle of "mother may I," IRTPA notwithstanding.

[2]

67123.049

2. In what areas has the Intelligence Community improved its integration and thus its performance?

Successive DNI's have developed noteworthy programs to drive integration of collection and analysis and to improve IC-wide performance in enterprise management, customer relations, information management, human capital, security and counterintelligence, mission management, procurement, and science and technology. While the impact of these programs has been uneven and while they represent a relatively small contribution to major IC accomplishments over the past five years, they are commendable efforts by the DNI to implement both the letter and spirit of IRTPA.

In my view, the performance of the US Intelligence Community, overall, has improved dramatically since 9/11. Analytic and operational tradecraft have advanced significantly. Performance in counterterrorism programs has reached the highest standard of professionalism and dedication. The application of technology has broadened, deepened, and accelerated. Interagency collaboration, especially in support of the warfighter, has improved markedly. And progress toward a more distributed model of intelligence support to users anywhere in the world is palpable and encouraging. The fusion of intelligence, the synergy of well-trained people and advanced technology, and the interagency teamwork in Afghanistan and Iraq are at their highest level ever — a level that seemed unattainable when I left government.

The creation of the DNI has contributed to this progress but other leaders and individual agencies — with Administration and Congressional support — also have taken impressive steps on their own. The Department of Defense (DoD) won Congressional approval to establish in 2002 the position of Undersecretary of Defense for Intelligence to improve management of its considerable intelligence assets and programs. Most significantly, in my view, the Secretary of Defense elevated the authority and boosted the budget of the Joint Special Operations Command (JSOC) to provide in the field a strong coalescing leadership, a clear chain of command, and a powerful authority to coordinate focused requirements for intelligence collection and analysis. I would risk the outside judgment that the cooperation of CIA, including its Counterterrorism Center, with the military has never been closer or more effective. While there is always room for improvement in the intelligence business, the strong, collaborative performance of our agencies "down range" today is unprecedented — and a source of justifiable pride for the IC.

3. In which areas of integration is improvement needed? Why do such gaps in integration remain — and are they due to inadequate DNI authorities, the DNI's failure to utilize authorities, or to other reasons?

The domestic picture is mixed. The key difference with "down range" is that there is no JSOC counterpart in the homeland to integrate intelligence processes and products. The FBI has built an impressive intelligence infrastructure and has shifted significant resources, once wholly devoted to law enforcement, to domestic intelligence collection and analysis. The National Counterterrorism Center is integrating foreign and domestic intelligence and analysis. The Department of Homeland Security, with its 22 constituent agencies sometimes taking initiative on their own, has made commendable strides in border security and some – but uneven –

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00424 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.050

progress in sharing threat-based information and coordinating policy with state and local governments and the private sector. Overall, however, domestic agencies do not show the strong unity of effort that is evident in theaters of conflict abroad. Domestic intelligence and security is a much slower work in progress. I would not assign significant blame for this to the DNI.

4. What is the status of the DNI's relationships with the CIA, DoD, and other entities, and how can they be improved? To what extent has Section 1018 of the 2004 Act, which requires that the DNI manage the Intelligence Community without abrogating the statutory authorities of the cabinet secretaries, been an impediment?

I believe that the DNI continues to pursue constructive relationships with key stakeholders to US intelligence — the IC, DoD, NSC, the Congress — but his efforts to establish legitimacy are hampered by the lack of clarity in his roles and responsibilities and by the perception of some that the DNI does not enjoy strong support from the Executive and Legislative branches. Within some components, the ODNI is viewed as another layer of bureaucracy without demonstrated value.

The requirement of IRTPA Section 1018, which requires the DNI to manage the Intelligence Community without abrogating the statutory authorities of the cabinet secretaries, is in the nature of self-evident "bumper sticker" guidance for any government agency head. It will not impede the DNI's progress, but neither did I see it as a vote of confidence by the Congress.

5. Has the DNI made effective use of the budget, personnel, and other authorities contained in the 2004 Act and E.O. 12333, as amended? If not, why not?

To the limited extent that I am qualified to comment on this, I would say that the DNI has pushed the envelope to execute his limited budgetary authorities and that his dialogue within the IC on the matter is dynamic and evolving. I have read that DNI Clapper and SECDEF Gates have made an agreement, important details of which are unknown to me, that would give the DNI "control" of both the National Intelligence Program and Military Intelligence Program. Potentially, this would be a major breakthrough giving the DNI budgetary authority spanning the whole IC. The agreement, however, would not have enduring significance until it has the force of a Presidential Executive Order or is embedded in law.

6. ***Does the DNI need additional authority? If so, what specific additional authorities are warranted, and why? For example, should the DNI be in the chain of command for covert action conducted by the CIA?***

The DNI likely will need additional authorities over time, but I would not make this a priority now. We need to take a big step back, reexamine IRTPA's assumptions, and seriously consider a new model for a DNI based on clear, discrete responsibilities that can be justified as value added for the 16 intelligence agencies and would be defended by the White House and the Congress. While I can argue from both sides of the covert action issue, I would give the DNI

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00425 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.051

only a consultative role here and have the CIA Director report directly to the President on what are often extremely sensitive issues involving the protection of sources and methods. In the larger scheme of things, this would not dilute the authority of the DNI to carry out his otherwise weighty responsibilities in the distributed leadership model I have described.

Looking ahead, I believe that the DNI position can be transformed to give it a legitimate, wholly constructive leadership role in the Intelligence Community, despite the obstacles that are now in the way. We should recall that IRTPA created the position after decades of controversy about the failure of successive DCIs to manage the Intelligence Community. To be successful, the DNI's roles and responsibilities need to be tied clearly to IC strategic priorities and requirements; stake-holder expectations of the DNI's performance must be managed within the context of the IC's time-tested distributed model of leadership; and it must be assumed that both the Executive and Legislative branches will back the incumbent in the exercise of his authorities.

The DNI should continue to improve IC-wide performance in such areas as information management, integration of analysis and collection strategies, human resources programs, and mission management. I would also identify seven strategic areas in which the leadership of the DNI would boost IC performance and strengthen US national security. The DNI should:

- ***Increase the focus on strategic, versus tactical, collection and analysis***: The IC needs to be able to "steal secrets" that matter for the long term and produce strategic, integrated assessments of foreign and domestic threats to US national security — assessments that can drive resources.

- ***Enable analysts to exploit the information age:*** I am confident that CIA analysts over the years have informed policymakers that the Arab regimes of the Middle East were generally corrupt, repressive, and threatened by youth bulges. Confronted by the Arab spring, however, I suspect the analysts had trouble playing catch-up ball because of their minimal access to the internet, social media, and outside experts.

- ***Strengthen the IC's commitment to science and technology (S&T):*** We are threatened today, more than ever, by technological surprise. The IC is too slow, in my view, to invest in internal scientific capability and in external relationships with experts.

- ***Boost IC Training and Education:*** The DNI is establishing a National Intelligence University. It should work to codify intelligence as a profession, strengthen interagency relationships, teach intelligence successes and failures, promote research, and convene the stakeholder of US intelligence from across the intelligence, policy, and congressional domains for constructive dialogue.

- ***Mature IC security and counterintelligence policies:*** The dramatic change to both the geopolitical and technical threats we face today represents a profound challenge to our security and counterintelligence policies. The DNI can assist the agencies to adapt their policies to the new fast-moving and complicated threat environment, and he is doing so. But this will be a work in progress for some time to come.

[5]

67123.052

- ***Continue to advance information sharing across the agencies.*** It is increasingly difficult for intelligence analysts to detect precise signals amidst overpowering noise. We have had notable setbacks in recent years. But the DNI has made measurable progress on this, despite the fact that the individual agencies own their own data.

- ***Rationalize and harmonize IC procurement strategies and policies — improve government performance in contract management.*** Easy problems to cite but among the hardest to solve. The DNI is positioned to make progress over time on this top priority.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00427 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.053

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"Ten Years After 9/11: Is Intelligence Reform Working, Part II?"
Homeland Security and Governmental Affairs Committee
May 19, 2011
As Prepared for Delivery

Good afternoon. Today we hold our second hearing on the topic: "Ten Years After 9/11: Is Intelligence Reform Working?" as part of our overall series of hearings this year on how well the security reforms enacted after 9-11 have protected our homeland security.

During our hearing last week, we explored a variety of issues related to intelligence reform. In contrast, this hearing will focus on a single big question – does the Director of National Intelligence have the authorities needed to lead our sprawling intelligence establishment?

I want to welcome our witness, former Director of National Intelligence Dennis Blair.

Admiral Blair is an extraordinarily talented and dedicated public servant who had an exemplary career as a senior military commander and a consumer of intelligence before agreeing to take on what we all know to be one of Washington's most challenging jobs – the DNI.

You are, of course, uniquely qualified to help us explore this issue.

I am grateful that you accepted Senator Collins's and my invitation to come and share your thoughts. Your testimony is in keeping with your career of national service and reflecting your extensive experience in national security matters.

We take your presence here today in that context. So thank you for appearing before this committee today and sharing insights into a subject you know well.

This Committee created the DNI as part of the Intelligence Reform and Terrorism Prevention Act of 2004 at the recommendation of the 9-11 Commission.

The Commission concluded that no one was in charge of the U.S. Intelligence Community and that this lack of leadership resulted in broad dysfunction and disunity that left us vulnerable to the 9-11 attacks.

The intelligence system that existed on 9-11 had been built to counter nation-states like the Soviet Union that had large bureaucracies and fielded massive armies of tanks, airplanes, and missiles that we sought to study and count.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.054

Intelligence collection and analysis could move at a slower pace, with each intelligence agency operating in relative autonomy, and still be effective.

But terrorists and cybercriminals today operate at Internet speed. To fight them successfully, we needed to change our system so we could be as flexible and nimble as they are. And it was to be the DNI's job to bring the necessary unity of command and effort to our 16 intelligence agencies, including the CIA.

So we ask: On a day-to-day basis, does the DNI have the authorities he or she needs to lead the Intelligence Community effectively? Does the DNI have the ability to forge the unity of effort across the community and achieve the level of integration that is necessary to meet the myriad of challenges that our nation faces?

These are the overarching questions we would like to pose today to Admiral Blair.

The intelligence reform legislation of 2004 gave the DNI authorities in critical areas including budget and personnel. Accordingly, we will ask your assessment of the DNI's use of these authorities.

For example, how often have DNIs been able use the DNI's budget authorities, and to what effect?

What impact have the DNI's personnel authorities had on the DNIs' ability to force greater integration of the Intelligence Community?

Are there gaps that DNIs have tried but failed to close due to a lack of some authorities? And are new authorities needed regarding budgets, personnel, or other areas?

Admiral Blair last testified before this committee in January 2010 in a hearing regarding the Christmas bomber, Farouk Abdulmutallab, who smuggled a bomb aboard Northwest Flight 253 that failed to detonate.

I remember being impressed that day that Admiral Blair and our other witnesses – Secretary of Homeland Security Janet Napolitano and National Counterterrorism Director Michael Leiter – all took their share of responsibility, admitted the system had failed, and told us that changes were already underway.

One of the questions I want to ask Admiral Blair today is if he was able to implement the changes he said were needed or if some of those gaps that allowed Abdulmutallab slip through the system still exist.

Let me close by saying that restructuring the government to meet new threats is hard and change comes slowly. When we passed the Intelligence Reform Act, we knew we would have to revisit the legislation to determine whether it needed to be improved in light of the evolution of the terrorist threat and other challenges facing our nation.

That's why we're here today.

67123.055

Statement of
Senator Susan M. Collins

"Ten Years After 9/11: Is Intelligence Reform Working? Part II"

May 19, 2011

The operation that tracked and killed Osama bin Laden demonstrates the kind of successful collaboration of intelligence and operations that we envisioned in reforming our capabilities and intelligence community in the wake of the attacks of 9-11-01.

This was a great victory for our intelligence efforts and a great blow to al Qaeda. But al Qaeda is not going away.

That is why it is time for Congress to examine and build on the successes since the Intelligence Reform and Terrorism Prevention Act -- which created the Director of National Intelligence. It is the opportune time to identify any shortcomings in that structure and work to correct them.

I look forward to hearing from Admiral Blair about what worked during his tenure as DNI, what didn't work, and what might be changed about the structure we designed seven years ago.

Admiral Blair is a fellow Mainer - hailing from Kittery, home of the Portsmouth Naval Shipyard. So, either coming from a great Navy town or following five generations of Naval officers preordained his career. We all hope he has a fine Navy Day here as we hear from him about his experiences as the DNI and his recommendations now with the benefit of 20/20 hindsight.

Almost 10 years since September 11 and seven years since our landmark legislation, we are safer but not yet safe. Our intelligence community is stronger and more effective than ever before, but plenty of turf battles remain. During his tenure, Admiral Blair was at the center of some unusually public battles with the CIA.

To help address lingering deficiencies in the Intelligence Community, the DNI must be the "quarterback" that the 9-11 Commission envisioned and we intended. At last week's hearing, General Hayden preferred the term "coach." I will be interested to hear whether or not Admiral Blair believes the DNI has been empowered to fill this critical role.

67123.056

At the first hearing in this series, the leaders of the 9-11 Commission, Governor Kean and Congressman Hamilton, agreed that presidential adviser John Brennan is, in many respects, performing the role we envisioned for the DNI when we authored the legislation. That troubles me, not due to any doubts about Mr. Brennan's capabilities, but because that structure undermines the statutory role of the DNI.

We must ask whether changes to the law are required, or whether it is simply a matter of more fidelity to the 2004 law to realize the potential of the DNI.

Admiral, thank you again for being here. I look forward to hearing your perspective.

Prepared Statement of Dennis C. Blair for the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Hearing entitled

"Ten Years After 9/11: Is Intelligence Reform Working? Part II"

May 19, 2011

The successful Osama bin Ladin operation would seem to be an occasion to celebrate the success of intelligence reform, not to criticize it. A decade of dogged pursuit of the man who launched the 9/11 attacks on the United States, involving the full resources of the Intelligence Community, finally found its man. The Intelligence Community then provided superb support to the Special Operations team that made the successful raid into Abbottabad.

It is commendable that for the single most urgent national security mission, when the objective is clear, the priority the highest, and the full attention of national leadership is engaged, the Intelligence Community works well together, and works well with the rest of government. It reinforces the importance of getting the system right, so that this kind of performance becomes the norm for all intelligence missions, so that the Intelligence Community operates routinely as an integrated team.

That was the goal of the Intelligence Reform and Terrorist Prevention Act (IRTPA) of 2004. IRTPA was passed in the wake not of a success, but of a disaster, and was an incomplete piece of legislation, passed under heavy time pressures, full of compromises and leaving many ambiguities. However the concept at its heart - integrating the activities of the sixteen intelligence agencies under a Director of National Intelligence - remains valid. There is a great deal of intelligence integration still to be done, and continued intelligence reform must continue as a national imperative. As I saw firsthand on many issues, with White House and Congressional support, the DNI can drive improvement in the Intelligence Community (IC) that will keep pace with the dynamic threats we face. I strongly urge this committee to continue to deepen intelligence integration by supporting a powerful DNI with a strong staff.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00432 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.058

How Intelligence Works

Intelligence support is a cycle; it begins with questions, whether from the President, a military commander or ambassador in the field or a domestic law enforcement agency: What is the status of Iran's uranium enrichment program? How effective or corrupt is a particular provincial official in Afghanistan? What is the threat to a city's mass transit system? The next step is for the intelligence agencies to collect information to help answer the questions.[1] Using the reports from the collection agencies, all-source analysts provide answers to the policymaker or operational official. If the intelligence collection is good, the answer can be detailed and specific. For example, if the head of a provincial reconstruction team asks about the reliability of a local official, and through signals intelligence, an NSA collector has retrieved records of bribes, then the analyst can provide a full and detailed answer. Lacking complete detailed information like this, the analyst will use his or her own expertise, fill in gaps with logical inferences, provide the best answer possible, and explain what is known with certainty and what is inference. This cycle of question, collection, analysis and answer repeats continuously. It involves officials in many different intelligence agencies collaborating by sending requests for information, reports of intelligence collected, and drafts of analytical judgments back and forth until an answer is provided.

Many improvements in this cycle happen through the individual efforts of the talented officers within individual intelligence agencies. However a decentralized, cooperative system will not meet the challenge of prying out the secrets the United States needs to understand that tyrants and terrorists are protecting by brutally enforced security measures as well as by denial and deception measures. Each agency will do the best it can, but none has all the capabilities necessary, nor the overall responsibility for the end result. Systemic improvement of the entire enterprise and tackling the toughest challenges are the unique responsibility of the Director of National Intelligence.

Assume there is an authoritarian country we suspect is developing a dangerous secret military program. Policymakers in Washington, combatant commanders and ambassadors in the field are asking for a detailed description of the program and the enemy's plan to use it.

It is difficult in closed societies to recruit a high-level program official willing to provide a continuous and detailed stream of information. It is more feasible to recruit a lower level, less dedicated and underpaid informant. If the lower level official can provide an e-mail address or phone number of a superior, then we can gain access to a stream of

[1] The major categories of intelligence collection are human, signals, geospatial and open source intelligence. Most of the funding of the major national intelligence agencies goes to collection: the National Security Agency (NSA) for signals intelligence, the National Clandestine Service (NCS) of the Central Intelligence Agency (CIA), the Directorate of Operations of the Defense Intelligence Agency (DIA) and the National Security Bureau of the Federal Bureau of Investigation (FBI) for human intelligence, the National Geospatial-Intelligence Agency (NGA) for imagery intelligence, and the Open Source Center (OSC) for intelligence available from public sources, in print or on the internet.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00433 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.059

communications that provides additional information. If that stream of information contains the location of a significant program site, then we can use imagery of the area for additional clues. Once we have identified an important site in the program, then we can recruit residents living nearby who can provide information on what is happening at the site.

This cycle of using clues from one intelligence source to cue entirely different collection methods repeats until a clear picture of the entire program emerges, with access established to the most productive human recruits, networks, and geographical facilities. In order for this close-knit cycle of tipping and cueing to occur, every collector and every analyst of a multi-agency team must have full access to all the relevant intelligence held by every other agency. Human intelligence specialists must be able to read not just the gist of a translated telephone conversation, but the full conversation in the original language. By the same token, signals intelligence specialists need to be able to read the full debriefings of human sources, not simply edited summaries.

Full sharing of intelligence at this level is not natural to individual intelligence agencies, with their understandable but sub-optimizing emphasis on the protection of information. Only the DNI and his office can institutionalize the building and empowerment of integrated interagency teams to integrate the skills of all the diverse agencies in the Intelligence Community to answer the most difficult and important intelligence questions.

The organizational approach to meeting the most difficult intelligence challenges is mission management. The job of the mission manager is to drive improvement in all aspects of the Intelligence Community's performance in an important intelligence area. A mission can be an individual country - North Korea, Iran, Afghanistan, Pakistan - or a crosscutting issue - combating terrorism or countering proliferation of weapons of mass destruction. Mission managers are senior intelligence officials chosen for their proven intelligence skills and for their community-wide outlook. As the champions of their missions within the Intelligence Community, they establish and evaluate the integrated collection teams I just described and develop plans for IC support to operations in the field. They write an annual assessment of the state of the mission and proposed plans for further improvement that feed into the budget development process.

When I became DNI in early 2009 I found that several of the mission management teams were working well, but that many others were struggling, and some did not even exist, even for high priority intelligence challenges. Working with agency leadership and my staff, I raised the visibility and priority of these efforts, and started a high-level review to assess progress, identify obstacles, set specific goals and ensure adequate resources were provided to these teams. Progress was steady.

My successor, Director James Clapper, has greatly expanded the concept of Mission Management, and there are now some sixteen National Mission Managers. I cannot tell if the expansion has been successful in improving the integration of intelligence collection and analysis for these missions. It was my experience that to be effective, a

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00434 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.060

mission manager needed the high-level and detailed support of the DNI himself in order to overcome the obstacles to integrated intelligence: agency restrictions on sharing of intelligence; agency control of personnel assignments to missions; agency control of budget execution. It took high-level attention and intervention to align agency priorities with overall national intelligence priorities. Perhaps over time the agencies will naturally support the mission managers, but it is not the case yet. It will be a challenge to the DNI and his staff to ensure that sixteen national mission managers are receiving the high-level support they need to be effective. Improved effectiveness will not happen without a strong and aggressive DNI.

Beyond organization and authorities there are two significant and encouraging trends in the Intelligence Community that are driving intelligence integration.

First, in the field, where it counts, I found that the level of instinctive cooperation across the intelligence agencies was high and enthusiastic. The officers in dangerous places doing tough jobs had no tolerance for bureaucratic obstacles. If an intelligence officer from a different agency had a skill or capability to contribute to the mission, he or she was expected to join the team. At one forward base a couple of years ago a CIA case officer was on the way to a restaurant to recruit an agent. An NSA signals intelligence officer intercepted a conversation about the final preparations to kill the American in that restaurant. A quick phone call to the case officer saved her life. Intelligence officers in the field are developing integrated intelligence operations well in advance of Washington.

Second, more than half of intelligence officers currently serving have joined since 9/11. The younger generation is much more instinctively willing to work with their colleagues from other agencies in collaborative, mission-centered organizations. They are much more impatient with bureaucratic barriers; internet-savvy, they are more likely to post and pull information from common databases rather than to hoard it.

The Role of the DNI

Each of the four Directors of National Intelligence since 2005 has faced a different set of challenges in integrating intelligence. Director Negroponte had to solve all the logistical problems of establishing a new organization and setting up basic organizations to carry out the responsibilities that IRTPA gave him. Director McConnell, a military intelligence officer by background, instituted a series of aggressive programs with specific objectives and deadlines to improve important aspects of intelligence operations, and led the revision of Executive Order 12333 which filled in several of the gaps in legislation. When I became DNI in January 2009, I inherited an Intelligence Community that was performing well in many areas, but still needed improvement. When I had gathered my leadership team, we wrote a new national intelligence strategy. It established four strategic goals for the Intelligence Community: Enable wise national security policies, support effective national security action, deliver balanced and improving capabilities, and operate as a single integrated team. This strategy guided my efforts during my time as DNI.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00435 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.061

Enabling Wise National Security Policies

The major forms of intelligence support to policy are the President's Daily Briefing, the six-days-a-week publication distributed to the top policymakers in Washington, and the intelligence papers and briefings provided to policymakers during the deliberations of the national security leadership at various levels.

As DNI it was my responsibility to ensure that there was a timely and accurate flow of intelligence information to policymakers as the Obama administration reviewed the policies it had inherited and took initiatives in new areas. I found that overall we had enough foundational intelligence information for smart, experienced analysts to present accurate and compelling explanations of the capabilities and intentions of countries and other groups the United States was dealing with. The Administration's Afghanistan/Pakistan policy deliberations have been described in detail in books and articles. The intelligence support to those deliberations was comprehensive, timely and realistic. Speaking truth to power was encouraged.

In fact, the appetite for intelligence was so strong in this Administration that policymakers often demanded a level of detail that we could not always provide. For example, we had high confidence that North Korea was pursuing a uranium enrichment program, based on the regime's own statements, physical evidence, and careful deductions from fragmentary evidence. However we did not have a complete picture of the nature and location of every component of that program. We had high confidence that Osama bin Ladin was holed up in the rugged terrain of the Afghanistan/Pakistan border region, but we did not know his exact location. As it turned out, he was a hundred kilometers away, closer to Islamabad than to Afghanistan. Like the Iranian regime itself, the Intelligence Community did not initially have detailed information on the nature and strength of the opposition that formed during the June 2009 elections.

It is the job of the DNI to push the Intelligence Community for better collection and sharper analysis on the important intelligence questions. However, it will always be the case that intelligence knowledge of the intentions and future actions of complicated, secretive authoritarian adversaries will never be known completely. The DNI must not only provide intelligence estimates, but also explain the limitations of intelligence and guide policymakers to take into account the range of uncertainties and limitations in intelligence judgments as they make policy decisions and establish programs.

Based on fragmentary intelligence and logical inferences, in the spring of 2009 I warned policymakers that al Qa'ida had the capability to conduct terrorist attacks using operatives with American passports or visas who had received training in South Asia and had returned to the United States. Policymakers understandably pressed hard for additional specific information, which was simply not available, despite our best efforts to identify individuals. It was not until they attempted to carry out their attacks that we learned the identities of Najibullah Zazi, Umar Farouk Abdulmutallab and Faisal Shahzad.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00436 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.062

The responsibility of the DNI in these cases, in addition to warning policymakers of the threat, is to work with responsible departments to develop security programs that take full advantage of the fragmentary intelligence information we could expect to gather. For too long the only responses to the incomplete threat information we collected on al Qa'ida operatives was a general color-coded nationwide terrorism warning or the "no fly" list. We needed to do better. I engaged personally with Secretary Napolitano on this issue, and her team early in 2010 and DHS developed several imaginative programs to take advantage of partial intelligence to guide their screening at border entry points. These programs are now in effect and achieving positive results.

The personal role of the DNI is crucial in these major issues. Some commentators have opined that the DNI can operate behind the policy scenes but not personally participate in the policy deliberations at the highest level. A regional or functional senior intelligence analyst, according to this line of argument, should attend the high-level policy meetings. Still others have the odd notion that the President's intelligence officer should give an intelligence assessment at the beginning of a policy discussion, and then leave the room. In fact, I was excluded from the final meetings in the White House that decided this administration's Afghanistan/Pakistan policy in the autumn of 2009.

These notions do the President and the country a disservice. It is the DNI, responsible for and knowledgeable of the intelligence judgments on major issues, the strengths and weaknesses of the organizations and individuals who formed those judgments, with the responsibility for allocating overall intelligence resources, and with the cabinet-level understanding of the country's and administration's needs, who must advise his fellow NSC members and the President on the big issues. He or she must be included in all the policy deliberations so that they do not stray from a realistic understanding of both adversaries and friends. He or she must work with other Cabinet officers to ensure that their intelligence support is as good as possible and is being put to the best possible use.

Supporting Effective National Security Action

Intelligence support for operations is different from support for policy in the amount and level of detail and short timelines. Military forces and civil teams in Afghanistan need to know where specific improvised explosive devices (IEDs) are buried, the identity and location of individual Taliban leaders and sympathizers, the competence of specific provincial leaders and the state of village economic development. Intelligence support to operations is technology-intensive, fast-paced, very specific and flexible.

In recent years with the major deployments of US forces to Iraq and Afghanistan, the largest volume of the nation's intelligence has been devoted to support these operations. There are other campaigns and day-to-day operations that require similar fine-grain, very current intelligence support: operations worldwide against leadership and operatives of al Qa'ida and other terrorist groups, Department of Homeland Security's screening of those entering the United States, and operations at home and abroad against international drug trafficking. All these important national security operational campaigns require very fresh, very detailed intelligence information to be successful. In recent years great

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00437 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.063

progress has been made in the quality and timeliness of this category of intelligence support.

In the office of the DNI, we had three important responsibilities in surging intelligence support to Afghanistan.

First was funding. Integrated support to operations requires a dense network of technical collection systems, high bandwidth communications, and intelligence centers; this system had to be built from scratch in Afghanistan. Analysts, collectors and communicators had to be sent forward and supported. We coordinated the development of this plan through the Intelligence Community Executive Committee[2], and gained approvals by both OMB and the Congress.

Second, my responsibility was to ensure that the intelligence was tailored to the requirements of Afghanistan, not copied from the template of Iraq or elsewhere. My staff and I worked to ensure that the non-military elements of the deployment to Afghanistan - the embassy team, and the provincial reconstruction teams - were able to receive the same quality of intelligence to conduct their missions as did the military units.

Third, it was my responsibility to ensure that intelligence was shared across all the organizations participating in Afghanistan operations, with the Afghanis themselves, and with our international partners. We continually pushed to share as much intelligence as possible, consistent with counterintelligence considerations. There were dramatic improvements that would not have happened without DNI authority and action.

Intelligence support to operations is the most integrated and effective of all the major intelligence activities. Go into any intelligence center involved in the campaign against al Qa'ida, or into a joint intelligence center in Iraq or Afghanistan, and you will meet officers from all the intelligence agencies, and often from many other countries, with high bandwidth, high security access to all the databases of their parent agencies, sharing with their teammates from other agencies in support of the mission of their organization. Most of them are young and have recently joined the intelligence community; for them this kind of integrated intelligence is a natural way of doing business. As they return to their parent organizations, and assume positions of greater responsibility, they will carry these habits of integration with them, raising the overall level of integration, and effectiveness of all the missions of the intelligence community.

Delivering Balanced and Improving Capabilities

A key and unique responsibility of the DNI is formulation of the budget for the Intelligence Community and approving major technical systems. When I arrived as DNI, there was no system in place to support major budget decisions with adequate analysis of costs, risks and alternatives, and there was a recent history of failed multi-billion dollar

[2] The Executive Committee (EXCOM) of the Intelligence Community, chaired by the DNI, is the regular meeting of the heads of the sixteen intelligence agencies and elements along with the senior staff members of the Office of the DNI. It is this body that advises the DNI on all major initiatives and decisions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00438 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.064

technical collection and information technology programs. Congress had justifiably placed hundreds of millions of dollars for one important class of technical collection system in an escrow account until we submitted a realistic plan.

One of my first actions as DNI was to convene an outside panel to review the Intelligence Community planning, programming, budgeting and evaluation processes, and the acquisition system. They did a splendid job, and I adopted all their recommendations.

The major missing component the panel identified was a program planning function to identify, analyze and decide the major, multi-billion dollar budget issues early in the budget process, leaving the smaller, multi-million dollar decisions for the end. In addition, the panel pointed out that there was no systematic process for identifying and analyzing system requirements; nor was there a program evaluation office to drive these essential functions.

We immediately created the office of Studies, Requirements and Analysis and staffed it without an increase in ceiling for the ODNI. The office was soon taking the lead in establishing a budget cycle and providing data and analysis to tackle many of the major resource challenges that faced us: the cost of retaining and storing data, overruns in major collection systems, older systems reaching the end of their service lives and needing replacement, and declining investment in science and technology. Within a few months this office was providing analysis of major budget and system issues for discussion in the Executive Committee with the entire Intelligence Community leadership before I made final decisions.

One area requiring major attention was science and technology (S&T), in which investment had been declining for several years. An excellent provision of the IRTPA was the establishment of the Intelligence Advanced Research Projects Agency - IARPA. This agency, modeled on the successful Defense Advanced Research Projects Agency, undertakes very risky technological developments that will have high payoff for intelligence. I increased IARPA's funding so that it could fund its most important initiatives, which were showing early promise.

However, S&T work within the major agencies needed attention as well. They had been able to adapt commercial systems for intelligence use in clever ways, but commercial products are often not suitable for intelligence use, especially in major technical systems. There had been no systematic program to develop the necessary specialized components. Under the leadership of a new team in the Office of the DNI, a system is now in place for S&T requirements and for assessing the performance of the agencies in meeting them.

A foundation has now been laid in the Office of the DNI for an analysis-based, coherent process to make overall resource decisions, including the acquisition of major technical systems. I was able to present a solid plan to Congress to release escrowed funding for the major technical collection system, and the program is now underway. There is now a system in place that has the essential important organizations and processes for the DNI

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00439 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.065

to carry out his responsibilities, but it will take continued attention and work to bring it to full effectiveness.

The DNI's role in resource management will be much more important in the future than it has been in the past. Since 9/11 the budget of the Intelligence Community has risen substantially, paralleling the increases in the Defense budget during those years. Tradeoffs are relatively easy to make under conditions of rising budgets. In the future, as budgets level off or actually decrease, it will be more important for the DNI to make the difficult tradeoff decisions and to be able to make those decisions across all the intelligence agencies, supported by deep analysis and a strong staff.

Unfinished Business: Organizational Issues

IRTPA, according to its authors and confirmed by my experience as DNI for a year and a half, was an incomplete step in achieving an integrated intelligence community. There are additional organizational steps that can be taken short of the more radical step advocated by some of forming an independent Department of Intelligence.

There are two fault lines that run through the structure created by the IRTPA - the relationship of the DNI to the intelligence agencies in the Department of Defense, and the relationship of the DNI to the CIA. There is also on occasion tension between the law enforcement responsibilities of the FBI and the intelligence responsibilities of the rest of the Intelligence Community.

Although located within the Department of Defense, which calls them "combat support agencies," I found that the National Security Agency, the National Geospatial-Intelligence Agency, the Defense Intelligence Agency and the National Reconnaissance Office provided top-notch support across government for both policy and effective action. There were at least two major reasons for this.

First, the traditional divide between military and national intelligence no longer exists. In all of the major national security challenges facing the United States, the military objectives and requirements have been intermixed with diplomatic and economic objectives and requirements. The major national intelligence agencies in the Defense Department realize they cannot separate military from civil objectives, that military success depends on an understanding both of the enemy order of battle and the political, cultural, economic and economic aspects of foreign countries; they support both military commanders and units and civilian officials alike with intelligence on all these aspects of the countries and groups the United States is dealing with.

Second, the leaders of the intelligence agencies in the Department of Defense are very broad in their backgrounds and outlooks. They are mostly all senior military intelligence officers with multiple joint operational assignments and first-hand experience in supporting different types of intelligence requirements. They know how to direct their agencies to support a full range of officials in Washington and the field. When I was DNI, I had no stronger teammates in the integration of intelligence across military and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00440 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.066

civilian requirements than Generals Keith Alexander and Ron Burgess, Admiral Bob Murrett, and retired General Bruce Carlson.

The major civil/military fault line I encountered was between the Department of Homeland Security and the National Security Agency in the area of cyber security, and I believe an organizational change would make a big difference in resolving it.

The National Security Agency has unmatched size and depth of expertise in cyber security, with the responsibility for protecting DoD networks. The Department of Homeland Security lacks this technical depth, but it has the responsibility for the security of the information networks of most of the federal government and also for the federal role in securing the information networks of the country's critical infrastructure.

DHS needs to draw on the technical skills of NSA to protect government and critical infrastructure information systems. However, there is strong opposition by many in the country and some in the Congress to any role for NSA in these civilian information systems. There is a suspicion that in helping DHS and private companies protect their networks, NSA will gain access to government and private systems to gather information on American citizens illegally. Based on my experience these fears are groundless, both technically and procedurally, but they are nonetheless real. I believe they could be surmounted by the designation of an NSA deputy to report in a dual-hatted relationship to the Secretary of Homeland Security for the purpose of cyber security for government and critical infrastructure networks. Safeguards, both procedural and organizational, could be established to ensure that NSA was not able to gather intelligence through its activities supporting DHS for information security.

A second area in which the relationship between the Intelligence Community and the Department of Defense needs to be improved is in operations against terrorists.

Currently operations against al Qa'ida and other terrorist groups are conducted as traditional military activities (TMA) by the Department of Defense under its Title 10 authorities. Direct action, led by the CIA, is conducted as covert action under Title 50. Over the past decade, the military officers and intelligence officials leading these operations have learned to cooperate well. However, the currently divided authorities take time and inordinate legal and staff work to work out chains of command, they result in one-off arrangements, and on occasion have caused delays in execution that could have resulted in missed opportunities. The operations would be even more effective if they were combined into integrated joint interagency task forces (JIATFs), whose commanders had both sets of authorities and whose staffs combined their expertise and skills. For time-sensitive operations against agile enemies, unity of command, and integration of capabilities is always more effective than stovepiped cooperation.

A new legislative basis for such a joint task force would be necessary - a "Title 60." Under Title 60, for operations against a terrorist group, for example Al Qa'ida in the Arabian Peninsula, either a senior CIA officer, or a senior military officer would command the task force, with the deputy from the other organization. The staff would

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00441 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.067

include both military and Intelligence Community officers. The task force would have the authority to use all the capabilities of both the Department of Defense and the CIA. It would gather intelligence both through intelligence agencies collection capabilities and military reconnaissance systems; it would command aircraft and drones – either DoD or CIA - for both surveillance and attack missions; it would command special operations strike teams and conventional military task forces; it would work directly with foreign military organizations and intelligenee organizations; it would recruit and train paramilitary forces under CIA authorities; it would draw on DoD strengths of planning, resourcing and conducted long campaigns; it would have the budget flexibility and contracting capability of the CIA to come up with quick and imaginative responses to immediate problems.

The Title 60 legislation would have to deal with some of the difficult issues that have kept Title 10 authorities separate from Title 50 authorities in the past. I believe that most of these issues are rooted in Cold War history, and are long overdue for change. For example, these operations would be secret, but would they be covert, that is, would they be conducted under the concept of plausible deniability? That concept, codified in Title 50, was a product of the Cold War, when the United States wanted to be able to take lethal action against the Soviet Union without the risk of escalation should the action be officially acknowledged. It is generally not relevant today for counterterrorist operations, often conducted in areas where weak states cannot enforce their own sovereignty. The raid that killed Osama bin Ladin was apparently conducted as a covert action under Title 50 – I can think of no operation in recent memory that was less intended to be plausibly denied.

Would military forces involved in these operations be subject to the Geneva Convention and enjoy Status of Forces protections? I believe they should. However in reality, the Geneva Convention is of little practical value when dealing with groups like al Qa'ida, al Shabaab and the Haqqani network in Pakistan.

Who would these task forces report to? Like joint commanders in the Department of Defense, these task force commanders would submit plans that would outline their objectives, their strategy, the resources they would require, and the authorities they would exercise. The plans would be fully staffed through DoD and the IC, and would be approved by the President after final staffing by the National Security Council staff. Then in execution, the task forces would report to the President through the National Security Council staff.

Finally, how would Congress be notified? I believe that these operations should be briefed to both defense and intelligence oversight committees. For one operation I can recall during my time as DNI we formed a team of DoD and IC members and explained the operation to the leadership of all four committees. That system worked well in that case, and could be used routinely.

The division of authority between the DNI and the CIA was difficult during my tenure as DNI. Before the IRTPA established the Director of National Intelligence, the Director of

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00442 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.088

the CIA had the additional job of Director of Central Intelligence, responsible for coordinating the activities of all the different intelligence agencies. In practice, most directors of the CIA found their time dominated by the responsibilities of running the CIA, and in interagency issues, it was the CIA that most often had its way.

Many individuals in the CIA understand the importance of intelligence integration and work constructively with other intelligence agencies and the new DNI organization in a team approach in which the CIA is important, but not necessarily dominant. However, often the CIA has used the leverage and influence it retained from its days of dominance to act independently, undercutting the authority of the DNI and attempting either to gain leadership of community intelligence activities or to act independently of them. The CIA often used its direct relationships with the White House and Congress and its relationships with the intelligence services of other countries for these purposes.

Most of the clashes I had with the CIA came when I challenged its separate means of influence and leverage. When, after careful and prolonged study and consultation, I signed a directive that specified that the CIA station chiefs would in the great majority of cases but not always continue to be the representatives of the DNI, representing the interests of the entire Intelligence Community in dealing with host countries, Director Panetta appealed my decision to the White House. When I attempted to direct a more disciplined approach to the formulation and supervision of covert action activities, the CIA continued to work directly with the National Security Council staff, arguing that any attempt to impose principles, standards and procedures on covert action would impair its effectiveness. In both cases, the White House worked out compromise solutions that left the CIA with a great deal of autonomy and weakened the authority of the DNI.

In addition, the CIA's basic organization acts against the wider national interest in integrated intelligence. It is a unique historical legacy that the national clandestine service, responsible for both recruiting spies and covert action, is in the same agency as the national analytical organization. In most other countries they are separate.

There are important disadvantages to the arrangement: The action-oriented, can-do culture of the national clandestine service dominates and sometimes intimidates the reflective, critical analytical culture of the directorate of analysis. To have the primary analytical organization in the Intelligence Community paired with the organization that gathers human intelligence makes less sense than it did in the past. While human intelligence will play an indispensable role in the future, a greater proportion of intelligence reports will be signals intelligence, gathered by the National Security Agency.

It is time to divide the CIA into two separate agencies - a human intelligence and covert action service, and a central all-source analytical agency - both reporting to the DNI.

For the National Clandestine Service, it is the gathering of human intelligence that should be its primary focus, with covert action a secondary mission. While right now the CIA is conducting a major worldwide campaign against al Qa'ida, this campaign will not

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00443 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.069

continue forever, and in time covert operations will return to their historically lower and more normal level. In addition, the sophisticated paramilitary capability within the Defense Department, developed since 9/11 by Special Operations Command, is better equipped than the CIA to handle prolonged paramilitary activities, which by their nature will not remain covert for long. Moreover, the Defense Intelligence Agency also gathers human intelligence, and its activities are closely coordinated with the CIA. It would make sense to combine its human intelligence officers into this separate human intelligence agency. Human intelligence provides absolutely vital context, and often-priceless detail for assisting policymakers to make the right decisions in Washington and helping operators in the field to be successful, and we need a separate agency for this mission.

For its secondary mission of covert action, a combined CIA and military national clandestine service should report to the DNI, rather than directly to the National Security Council staff, keeping the DNI and appropriate staff generally informed, as is now the case. Covert action programs under the supervision of inexperienced National Security Council staffers have been the cause of major setbacks to American national security interests when they have gone astray. The President with the assistance of his staff should approve them and be kept informed of their progress, but the responsibility for supervising them, assessing them constantly for success or danger signals should be the responsibility of his confirmed principal intelligence officer, the DNI.

Those who argue against this arrangement cite the importance of secrecy, flexibility, speed and responsiveness of the direct CIA-White House link. These qualities are exactly what have caused disaster in the past, from the Bay of Pigs to black sites. Another layer in the chain of command need not add delay, and can provide constructive supervision and protection of the country's and a President's long-term interests. The Department of Defense conducts equally quick, flexible and sensitive special operations under the Secretary of Defense and his staff without the Special Operations Command reporting directly to the White House.

The Directorate of Analysis of the CIA is the most capable all-source analytical agency in the intelligence community. Despite the major well publicized mistakes in analysis that the CIA has made, most recently the National Intelligence Estimate on Iraqi Weapons of Mass Destruction, policymakers with good cause and for many years have valued the analytical skills, databases and deep expertise of the CIA. A separate, all-source analytical agency reporting directly to the DNI would be a very positive step. As part of such reorganization, part of the all-source analytical capability of the Defense Intelligence Agency should be incorporated into this organization. As explained earlier, the previous distinctions between national and military intelligence have been erased with the end of the Cold War, and to combine military and civil analysts into a single all-source analytical organization that would support both civilian and military policymakers and operations in the field would be a major step forward.[3]

---

[3] The Defense Intelligence Agency funds and manages most of the specialized analytical support of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the combatant commanders and other officials and offices in the Department of Defense. These analytical resources should remain in DIA.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00444 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.070

Unfinished Business: Cyber

The explosive growth of information technology affects the Intelligence Community more than any sector of the national security system.

First, the information revolution has affected intelligence collection. By sheer volume, it is the National Security Agency that collects and publishes the most intelligence, and the proportion is constantly increasing. The three challenges in this area are (1) gaining access to the databases and communications locations where the most valuable intelligence can be collected, (2) storing the huge volumes of information collected, and then (3) sorting out the important from the background information.

Despite the difficulties of access, volume, and relevance, there have been countless successes in collecting information to save American lives and inform American policies. However, the volume of information and complexity of the global communication system are continuing to grow exponentially, as are adversary defensive measures. We need to work harder to maintain the same access and understanding.

My primary responsibility in this area was to ensure adequate funding for developmental programs to ensure continued access and better capabilities to overcome adversary protective capabilities, store information, and sort the important intelligence insights from the background information. Continued major investments will be necessary.

The second major area in which the Intelligence Community has been powered by the information revolution has been in access and collaboration. Today's intelligence analyst has better access to the work of predecessors and to colleagues and greater ability to interact with those whom he or she supports, than ever before. Analytical jobs that took weeks can be done in hours. We are adapting many commercial tools and building our own. When I became DNI, there was an Analysis Space project known as A-Space on which communities of interest of intelligence analysts spontaneously formed around tough questions. In addition, a major effort was underway to store all finished analysis by all agencies into a single electronic Intelligence Library and to make all this intelligence analysis available to all authorized users. The challenge was to build a system of authorizing users and to ensure that there was adequate audit capability to detect misuse.

The drive for continued progress and to develop new ways to collaborate, share information, and interact across agencies is uniquely the responsibility of the DNI. Like so many desirable improvements to the overall intelligence community, there is little incentive for an individual agency to take the initiative or spend the resources to advance the common good - it is up to the DNI to take the lead.

The third area in which the information revolution profoundly affects the Intelligence Community is counterintelligence. The United States keeps more of its classified information in electronic databases, accessible by more communications networks, than any other nation. Our adversaries know it, and more and more of their espionage efforts

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00445 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.071

are to penetrate these networks and databases. Their capabilities go from simple hacking on the Internet and recruiting American officials with access to implanting trapdoors at the chip and operating system level. The Director of National Intelligence is the country's chief counterintelligence officer, responsible not only for protecting our intelligence information, kept in the networks of the Intelligence Community, but for stopping foreign espionage organizations from stealing any of our secrets - military, diplomatic, economic.

Coming into office in 2009, I found that our counterintelligence capabilities fell short. I convened a special advisory panel chaired by former Director of the FBI Louis Freeh. This panel made a number of very useful recommendations, and I implemented all of them. As I left office, I felt much better about our capability and about the prospects of being able to defend our systems against foreign espionage, but this is an area that requires continued attention and effort. There is no ultimate solution, no hardware or software system that will be impenetrable. The only answer is a continuing counterintelligence effort by very skilled intelligence officers, adequate resources, and continued DNI attention and emphasis.

There is a final cyber area in which there is important policy work to be done - computer network attack. It was one of the more difficult and frustrating subjects of my time as DNI.

The specific details of the computer attack activities and capabilities of the Intelligence Community are classified. However it is both possible and important to understand the principles involved at an unclassified level. The United States needs to decide when and how to employ this potentially effective means to defend itself.

Our adversaries are using the internet against us – jihadist web sites spew anti-American venom and encourage suicide attacks; al Qa'ida operatives use the internet for surveillance of American targets, planning of attacks, and communications to conduct the attacks. If the Intelligence Community has the capability to stop or slow down this activity, we should do so.

However, determining the legally authorized basis, the responsibilities within the government, and the process for planning and conducting these attacks is far from settled. Because the global communications system is so new, interconnected among foreign and American persons and companies, and continually evolving, the Department of Justice has been unable to provide a practical and durable legal basis for computer network attacks. They do not fit into the established categories of either traditional military activities or covert action. Computer network attacks can cause collateral damage, from slowing or denying internet service to many users to permanent damage to computer control systems, and the internet is so complex it is difficult to predict all the collateral damage in advance with precision. It is not surprising that the US Government has moved slowly.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00446 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.072

The problem is that the technology and our adversaries are not similarly inhibited and that we risk falling behind both the threat and the opportunities. Both in the Executive Branch and in the Congress we must develop working approaches to computer network attack and learn as we go. We cannot wait for complex legal opinions that are impossible to turn into real operational capability; we cannot decide on roles and missions on the basis of bureaucratic rivalries, and we need to experiment with low-risk but useful operations to build the capability and the understanding to take full advantage of this powerful capability. The Director of National Intelligence, as well as the Secretary of Defense and the Attorney General, must drive this issue, which ultimately will require White House decisions and Congressional authorization.

Unfinished Business - National Intelligence

Our border defines the responsibilities of American foreign-oriented intelligence agencies on the one hand, and domestic law enforcement and security agencies on the other. Intelligence agencies, with rare and carefully authorized and supervised exceptions, do not operate within this country. They do not spy on Americans. The domestic government agencies operating in the United States and authorized to investigate American citizens[4] protect Americans under well-established procedures for safeguarding their privacy and civil liberties.

Al Qa'ida and its affiliates have members, "wannabes," and sympathizers in the United States, who travel into this country to conduct surveillance, plan attacks, and carry them out, and are increasingly using American citizens and U.S.-based information systems in their planning and operations. These deadly enemies of the United States flow freely across our borders.

The government-wide challenge that 9/11 so tragically illustrated is to detect and track threats to the United States through the integration of the geographically defined capabilities and activities of all intelligence and law enforcement organizations. A great deal of progress has been made since then to share information. In the case of David Headley, for example, the American who was allegedly involved in planning the LeT attack in Mumbai, the FBI and the other intelligence agencies shared information and coordinated actions smoothly and quickly. A careful review of the nearly successful Christmas Day 2009 bombing over Detroit concluded that information was shared among intelligence agencies.[5]

One of the most important authorities given to the DNI in IRTPA is the responsibility to define what constitutes "national intelligence" under the guidance of the Attorney General. Under this authority, the DNI can designate information collected anywhere

[4] Law enforcement organizations with major intelligence capabilities include the FBI, the components of the Department of Homeland and Security and state and local law enforcement organizations.
[5] The failure to identify Abdulmutallab before he boarded the flight to Detroit was due to a combination of mistaken leadership decisions on assigning analysts to the threats coming out of Yemen, technical limitations of information systems, and the difficulty of picking out the important clues from the great torrent of data engulfing analysts.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00447 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.073

within the federal government as national intelligence, which means that it can be shared with all other intelligence agencies and used in analyzing threats to the country.

The most valuable national intelligence is the huge collection of databases of routinely collected government information that can be searched by computer algorithm. For example, an analyst may know that a potential terrorist attacker with the first name of George is between 23 and 28 years old, has lived in Atlanta, Georgia, recently, and has traveled often to Yemen. That analyst would like to be able very rapidly to query the travel records of the Customs and Border Protection Service, the investigative records of the Atlanta Police Department, the visa records of the State Department, and dozens of other government databases to learn George's full name, current location, and whether he has been involved in any other suspicious activity. Right now our analysts can conduct some of these database searches, but not all; some are one-click operations, but many are very complicated. The algorithms available to help in that search are inadequate to the volume of data that must be screened.

Despite these difficulties, there is a great deal of sharing of intelligence and information across the foreign intelligence/law enforcement divide, and progress is made every month. The FBI contributes thousands of intelligence reports to counterterrorism databases every year, and state and local law enforcement organizations also forward suspicious activity reports to NCTC and other organizations. However, we are still far from the point at which an intelligence analyst can quickly and easily find all relevant information with a single query.

Expanding the scope of national intelligence raises important privacy and civil liberty concerns. Government officials at all levels collect enormous quantities of information about Americans and visitors to this country in the course of doing their jobs. Should this information be readily available to intelligence analysts so that they can ferret out the few Americans who threaten the rest?

It is the responsibility of the DNI to use his existing authority to the fullest and to make the case for additional sharing, under careful privacy and civil liberty safeguards, to protect the overwhelming number of law-abiding Americans from the few who either cooperate with foreign organizations or are inspired by them to kill and harm. It is also the responsibility of the DNI to provide the resources and drive the technology of improved sharing and searching of the huge amount of data available so that the limited number of analysts can find the key pieces of information and put them together.

I did not have enough time as DNI to widen the definition of national intelligence, to increase the timely flow of information among foreign intelligence and domestic agencies, nor to improve the technical means to do so. We made important progress after the December 2009 attempted bombing of an aircraft over Detroit, but there is much more to be done.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00448 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.074

As with so many additional steps required in intelligence reform, a strong and aggressive DNI, with support from the White House and Congress, is necessary for progress.

Unfinished Business: DNI Authorities

The direction for continuing intelligence reform for the United States is clear: a more integrated but still federated system led by a strong Director of National Intelligence supported by an experienced and innovative staff.

As DNI, I could have led this process had I enjoyed the support of the President and his staff. However, their past experience, priorities, and the White House-centric style of national security governance never offered me the opportunity.

With a supportive White House and Congress, however, real possibilities open for progress. Most of the authorities to continue integration already exist either in the IRTPA or in the implementing Executive Order 12333. However, several additional authorities for the DNI in the areas of personnel and budget and the ODNI staff would speed integration:

Personnel

Senior personnel appointments in the intelligence agencies are one of the keys to successful integration. The joint duty provision of the IRTPA makes it mandatory that an intelligence officer completes an assignment outside his or her parent agency to be promoted to the senior ranks. This provision will raise the overall level of joint commitment by senior leadership, but there needs to be individual consideration of the very top leaders.

The IRTPA requires the concurrence of the DNI for the appointment of the top leaders of all the sixteen intelligence agencies or entities. I recommend that the concurrence of the DNI also be required for the second- and third-level positions. It is these officials who are the keys to integrated intelligence once the top leadership has set the direction. The DNI needs to ensure that there are community-minded officers leading the individual intelligence agencies. This provision could be established either by legislation or by executive order.

The director of the CIA is a special case. The IRTPA grants the DNI the authority to recommend the CIA Director to the President. In practice this has been the case only once, when DNI Negroponte recommended General Michael Hayden as the CIA Director. In 2008 the President-elect consulted me in the process of naming a CIA Director, but the input of his campaign staff was more important than mine.

The CIA Director (or the directors of the two organizations I recommend take the place of the CIA) should be a career officer and serve for a fixed term. The CIA is a complicated, sensitive organization, and an officer who knows it from years of service,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00449 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.075

has credibility and an instant following in the organization, yet has ideas for how it needs to improve and work with the rest of the Intelligence Community, would be the best leader. Historically, experienced CIA officers have been among the best directors - Robert Gates, William Colby, Richard Helms. A professional CIA Director concentrating on running and improving the Agency would more likely work more smoothly with a DNI who brought outside skills and perspectives. There are several senior CIA officers in the Agency right now with the potential to be outstanding directors.

I recommend legislation mandating that the CIA Director be a career CIA officer recommended by the DNI and appointed by the President for a fixed term, and that the CIA be split into an all-source analytic agency and a clandestine and covert service, both headed by career officials appointed for a fixed term and under the DNI's direction, authority, and control.

There is a single sentence in the IRTPA stating that the Director of the CIA "shall report to the Director of National Intelligence regarding the activities of the Central Intelligence Agency." This sentence needs to be strengthened with specific language specifying that the Director of the CIA submit plans and reports on all its activities to the DNI for approval before they are provided to the White House or to Congress, and that the Director of the CIA will seek the approval of the DNI for significant communications with the intelligence services of other countries. It was in these areas that I found that the CIA exercised a degree of autonomy that both undercut DNI authority made policy without formal consideration of the DNI or the National Security Council.

Budget Authority

The authors of the IRTPA thought that they were providing the DNI with one of his most powerful tools in his budget authority. The reality, like much of IRTPA, is that the tool has not been used to its fullest, and is limited.

One reason budget authority has not been exercised has been that the growth of overall intelligence funding over the past 15 years has made financial discipline unnecessary. It is likely that budgets will be much more constrained in the future, and tradeoffs essential. Another reason has been the lack of a strong analytical capability to support budget decisions. As described earlier in this article, by the time I left the DNI post, there was a planning and programming capability in place.

The DNI and his Chief Financial Officer have less authority than the Defense Department's Secretary and Comptroller. If we are to have an integrated Intelligence Community, then it will be essential that the DNI have a comparable level of authority.

I recommend giving the DNI full comptrollership authority. This would mean that agency heads could not bypass the ODNI in dealing with either OMB or with the congressional authorization and appropriations committees. Of course there would be information flow

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00450 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.076

between the agencies, OMB, and Congressional staff, but it would require discipline by OMB and the committee staffs always to deal through the DNI.

With full comptrollership authorities, the ODNI could use budget resources effectively across the community. There are many cases in which money should be moved from one agency to another in order to solve common agency problems. The DNI has rarely been able to accomplish this function, especially in the year of execution, and then to monitor and enforce successful solution of the problem. The only way in which common agency problems have been solved is with additional money granted by the Congress. The agencies are in the habit of requesting additional budget allocations when receiving assignments. An Intelligence Community comptroller would simply move the money based on the best analysis available and DNI decisions.

For example, if the DNI designates the CIA the executive agent for network audit capability within the Intelligence Community, there should be an implementing fiscal plan that takes the resources currently being spent on this function from the other agencies and transfers them to the CIA, which would then be responsible for the delivering the audit capability. Budget-based transfers like this are a rarity now, but they will be crucial in the future as overall intelligence funding is reduced, as seems likely.

I recommend that Congress grant and OMB directives confirm the DNI's authority to transfer National Intelligence Program funding across agencies throughout the budget cycle.

Finally, I recommend transferring the funding under the military intelligence program (MIP) in the Department of Defense budget to the national intelligence program (NIP) in the DNI budget. Before I left, James Clapper, then the Undersecretary of Defense for Intelligence (USDI), and I made great strides in coordinating the MIP/NIP actions. For example, we split-funded several important programs, issued a single planning guidance document, and included both Defense and the Intelligence Community in major studies. However, the MIP is subject to DoD decisions that have nothing to do with intelligence - the OSD Comptroller can subject it to overall DoD taxes, or can overrule agreements that have been worked out between the DNI and the USDI. There still would be cooperation between DoD and DNI on many classified programs, but the funding for intelligence should all come through the DNI and the national intelligence program.

History is not a good guide to the importance of these provisions. In the recent past, with growing budgets, DNI concurrence has been required on supplemental budgets, reprogramming, and the major budget actions. However, in practice, the authority has been largely to shape and approve agency initiatives. In future, as budgets level or decrease, it will be time to enforce tough choices, and this is where the DNI authority will be important.

In Conclusion

2011 is the right time to strengthen the national commitment to an integrated intelligence community, led by a strong DNI supported by a skilled staff. The groundwork for this progress has been laid in the past five years, and the future steps needed are clear. I urge this committee to strengthen the 2004 Intelligence Reform and Terrorism Prevention Act of 2004 to make a good Intelligence Community even better.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00451 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.077

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
Homeland Security and Governmental Affairs Committee
June 22, 2011
As Prepared for Delivery

Good morning and welcome to our hearing today where we will discuss the security of our rail and transit systems and strategies for the future to improve the defense of these systems, which are historically open, and, therefore, in this post 9-11 world, vulnerable.

This hearing is being held as part of a continuing series of hearings and investigations our Committee has committed to do during this year, as we approach the tenth commemoration of the attacks against America on 9-11. But in this particular case, this hearing was also catalyzed by the reports from the raid on bin Laden's compound, which yielded documents apparently indicating that Osama bin Laden continued to urge members of al Qaeda to attack the rail sector of the United States, particularly on or about the tenth anniversary of September 11. One of those apparently included a plan to derail a train. Some of the analysts we've talked to have concluded that the most likely form of this attack would be multiple operatives acting independently against separate targets as part of a coordinated attack on one system, of course, usually at peak travel times. There's also been a reference to bin Laden suggesting that these kinds of attacks might be carried out most dramatically on rail lines over valleys or bridges. In other words, this again made real the threat to our rail and transit systems, a threat we've seen carried out in other places: Mumbai, the first attack, Madrid, London Moscow, and of course plans that were thwarted right here in Washington D.C. and New York City. In fact the Transportation Institute issued a report that found since September 11, 2001, worldwide, 1,800 attacks have been carried out on surface transportation, mostly buses and trains, obviously not all of them major, causing over 3,900 deaths. Compare that to the 75 attacks carried out on airplanes and in airports that caused 157 deaths.

Add to that the fact that 14 million people use these systems every day. In Connecticut, the Metro North New Haven line is one of the busiest rail lines in our country.

Speed, reliability, and convenience are hallmarks of mass transit, and we support mass transit as part of broader societal goals. But with so many passengers at so many stations, along so many paths, these systems are very difficult to secure. We certainly haven't gone without security. Since 9/11 we've increased the level of surveillance cameras, explosive detection dogs, security teams, and, of course, greater public awareness. Secretary Napolitano and Transportation Security Administrator Pistol have energetically promoted the "See Something, Say Something" public education campaign because the security of our rail system does hinge, in large part, on the awareness and actions of an observant citizenry. But a decade after 9/11, as one of our witnesses, Dr. Stephen Flynn, directly suggests, we've got to move beyond "See Something, Say Something" to "DO something."

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.078

On transit security, of course, traditionally the responsibility belongs to state and local officials, but in our time, the Transportation Security Administration (TSA) has played a critical role. TSA has been working with state and local governments to improve rail and transit security and now has 25 mobile security teams -Visible Intermodal Prevention and Response or VIPR, one of the best acronyms that I think our government has - it sends into the field. The President's Fiscal Year 2012 budget requests 12 more of these teams. TSA also has 320 security inspectors working with local transit officials to assess the security of trains, platforms, and rail yards.

But there is much more TSA and state and local governments can and, I think, must do.

Let me just mention a few. First and foremost, TSA really needs to fulfill a 2007 legislative requirement to develop uniform standards for rail and transit training programs, for background checks for frontline employees, and for transit agencies' security plans.

Second, the Department of Homeland Security (DHS), I think, should step up its efforts to develop creative, non-intrusive transit security solutions – especially to detect improvised explosive devices – which history has shown are the weapons of choice for disrupting rail and transit systems. As you know the Department of Homeland Security has a Science and Technology Directorate explicitly to achieve purposes like this, but specific R&D on rail and transit security innovations, in my opinion, has been much too limited.

Third, TSA, I think, has to improve its intelligence sharing with state and local officials. It's come a long way, but it needs to come further, and also with the private sector too, and provide information that is both current and useful to them that is in some sense simplified and easier to manage.

Fourth, all of the stake holders in transit security need to be conducting more training exercises to accustom rail and transit officials with the unique requirements of disaster prevention and response involving mass transit, particularly trains. So I hope TSA and FEMA will continue to expand these exercises, and local authorities and state authorities will become more proactive and ensure that employees at every level are involved.

And fifth, we've got to continue to work with passengers to make them full partners in securing our rail and transit systems. That includes educating them about the risks, reporting suspicious activity, and how to respond should an attack occur.

We have the DHS's Transit Security Grant Program, through which approximately $1.8 billion in rail and transit grant funds have been distributed since 2006. These funds are really critically important to our state and local authorities, and that's why I feel that the House action to zero these funds out is just plain bad policy and I hope we will be able to overturn that here in the Senate.

I do want to stress that our law enforcement and intelligence agencies have successfully thwarted plots against rail and transit systems and, in talking about what more we can do, we cannot move forward without acknowledging the remarkable work done to thwart the 2009 plot by Najibullah Zazi to explode suicide bombs in the New York subway system, which was disrupted by brilliant intelligence and law enforcement work. A threat to the D.C. metro system last year was similarly uncovered and stopped before anyone was hurt. So these are the subjects I want to take to our witnesses. We really have the best in the field before us, and I thank them for their commitment to strengthening the security of our rails and mass transit systems and to being with us today.

67123.079

United States Senate
Committee on Homeland Security and Governmental Affairs
Senator Susan M. Collins

Contact: E.R. Anderson
202-224-4751

Statement of
Senator Susan M. Collins

As Prepared for Delivery
See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit

June 22, 2011

★ ★ ★

It is a pleasure to welcome back Administrator Pistole to our committee. It has been almost a year since his confirmation, and I appreciate his commitment to strengthening the safety and security of our transportation infrastructure and travelers. I'm also happy to see Commissioner Boynton here from Connecticut to lend his perspective from the state level and Stephen Flynn, who has provided this Committee with his insight on homeland security issues in the past.

Today's hearing on rail and transit security is timely. Only a few days after our U.S. Navy SEALs killed Osama bin Laden, the Department of Homeland Security and the FBI released an alert about rail security. The information was dated from early last year and was not connected to any particular city or rail line; nevertheless, it demonstrated that mass transit remains a terrorist target.

Soon after 9/11, terrorists began targeting mass transit systems. On March 11, 2004, 10 bombs exploded on four commuter trains heading into central Madrid. The attacks left 191 people dead and 1,800 wounded in what is regarded as the worst Islamist terrorist attack in European history.

The U.S. has been subject to rail plots as well. Since 2004, the U.S. Government has thwarted five terrorist plots against our nation's transit and rail systems. Metro and subway stations in New York City, Washington, DC, and train tunnels between New York and New Jersey were the intended targets.

While improvements have been made since 9/11, the challenge of securing rail and mass transit systems is enormous. As CRS reported in February, passenger rail systems, primarily subway systems, carry "about five times" as many passengers each day as do airlines, over many thousands of miles of track, and serving hundreds of stations that are designed for easy access by passengers. The vast network and sheer volume of riders make it impractical to conduct airline-type screening.

Security at airports is now the responsibility of the federal government, but security at subway, bus, and rail stations is largely in the purview of mass transit providers in partnership with state and local governments.

It is vitally important that the federal government, in concert with local partners, help to ensure the transit providers and local officials have the equipment and training to plan for and respond to terrorist threats -- while ensuring taxpayer dollars are spent efficiently.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00454 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.080

In addition, federal agencies must partner with state, and local law enforcement to develop a process to identify and report suspicious incidents and share that information nationally, so it can be analyzed to identify broader trends.

GAO recently reported that transit administrators and public transportation professionals currently receive security information from a variety of sources. Nearly 80 percent of respondents used five mechanisms or more to receive security information. Additionally, through interviews with public transit agencies of various sizes around the country, GAO identified at least 21 mechanisms through which these agencies received security-related information. DOT's Federal Transit Administration, TSA, the American Public Transportation Association, and public transit agency officials interviewed "expressed a desire to streamline information sharing to reduce the volume of overlapping information public transit agencies receive."

As we work to improve and streamline information sharing, we need to remember that an alert citizenry remains our first line of defense against terrorist attacks, whether at transportation hubs or city parks or Times Square.

A good example is how an alert street vendor, noticing smoke coming from a vehicle in Times Square, reported it to local law enforcement and thus helped to disrupt the attempted bombing. If not for this concerned citizen, the consequences could have been deadly.

In 2007, Senator Lieberman and I coauthored a law that made it easier for alert citizens to report suspicious activity in the transportation sector indicating potential terrorist behavior without the threat of frivolous lawsuits. This year, we reintroduced our "See Something, Say Something" legislation to expand those protections to reports of such behavior in all other sectors. I hope the Administration will endorse this legislation.

The world is a safer place without Osama bin Laden, but we are not yet safe. We are better prepared for terrorist attacks across all modes of transportation, but future attacks – at least attempts – are certain. The enemy continues to innovate and test our defenses.

Administrator Pistole and I recently spoke with the U.S. Chamber of Commerce about these challenges. We agree that one of our greatest assets in this effort is the spirit of innovation and flexibility that are fostered when we partner with state and local government, local law enforcement, and the private sector. We are able to benefit from their eyes, ears, and ideas.

I thank our witnesses for being here and look forward to our discussion.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00455 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.081

Statement of Senator Mary Landrieu

See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit

June 22, 2011

Thank you, Mr. Chairman and Senator Collins for calling this important hearing on rail and transit security. According to evidence discovered at his compound in Abbottabad, Osama Bin Laden was plotting a major attack on U.S. transit systems in the months preceding his death, and intelligence officials believe that branches of Al Qaeda may be doing so still. Terrorists carried out devastating attacks against transit systems in Madrid (in March 2004), London (in July 2005), and Mumbai (in November 2008). Since 2008, three men have been arrested in separate plots to attack the Long Island Railroad, the New York City subway, and the Washington, DC metro. And just 11 days ago, Amtrak announced an incident of intentional switch box tampering in Iowa that is now under investigation by the FBI. According to the American Public Transportation Association (APTA), only 50% of local transit agencies meet the 22 security standards it established in cooperation with TSA. In other words, terrorists are actively targeting our rail and transit systems, and our level of preparedness is fall short of where it needs to be, so we must focus resources to address this looming threat.

As Chairman of the Homeland Security Appropriations Subcommittee, I am in the process of writing legislation to allocate funding across the Department in Fiscal Year 2012 and provide support to high-priority programs that keep us safe. Unfortunately, the House of Representatives has sent over a spending measure for FY12 that would increase the nation's vulnerability to attacks on our rail and transit systems, by reducing funding for grants, research, and response teams.

- Grants - The House bill cuts preparedness grants by 60%, including grants for transit security ($245m in FY11). The Transit Security Grant Program (TSGP) supports drills and exercises, training, canine teams, anti-terrorism teams, and infrastructure hardening.
- R&D - The House bill cuts Science & Technology funding by 35% compared to FY11 and comes in 54% below the President's request. S&T's Rail and Transit Security team has ongoing projects with TSA right now that are focused on enhancing security assessments, assessing and hardening infrastructure, conducting underwater surveillance of tunnels and bridges, and evaluating the use of Closed Circuit Television (CCTV) to detect abandoned baggage and identify its owner. S&T was also responsible for developing the PROTECT Chemical Incident System that has been deployed in the New York, Washington, and Boston transit systems. A cut of this magnitude would force the Department to scale back and eliminate numerous rail and transit security research initiatives.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00456 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.082

- VIPR Teams - The House bill fails to include funding for 12 Visible Intermodal Protection and Response (VIPR) teams that was requested by the President to augment transportation security ($26.8 million for 12 teams and 331 FTEs). In the first half of FY11, 70% of VIPR team deployments addressed threats to surface transportation, with the vast majority focused on mass transit. Teams are usually deployed at the request of local transit agencies to conduct patrols and establish random security checkpoints, and they consist of Surface Transportation Security Officers, explosive detection canine teams, Behavior Detection Officers, and state and local law enforcement.

Without adequate resources, the Department of Homeland Security cannot address this threat. So as the Senate proceeds to consideration of spending legislation for the Department, I would urge my colleagues to reject the House's irresponsible cuts to programs such as these which support rail and transit security.

The passenger volume and physical design of train and subway stations require a unique security approach that is different from the one we employ at our nation's airports, seaports, and land Ports of Entry. It must be efficient, multi-layered, and based on risk. TSA has engaged the public through its "See Something, Say Something" campaign and improved information-sharing with local transit authorities and law enforcement agencies. But it must also issue overdue standards for employee training in evacuation procedures, protective equipment, and detection, as well as metrics for overall transit system security. Adequate funding and program delivery improvements such as these are vital to securing these transportation networks and deterring, preventing, and mitigating the consequences of a terrorist attack.

I thank the Chairman, and look forward to the witnesses' testimony.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00457 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.083

Statement of John S. Pistole

Administrator

Transportation Security Administration

U.S. Department of Homeland Security

before the

United States Senate

Homeland Security and Governmental Affairs

June 22, 2011

Good morning, Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) surface transportation programs.

As you know, TSA's efforts in the surface transportation domain are undertaken to reduce security vulnerabilities and to strengthen resilience against terrorist attacks. In this domain, which includes mass transit systems, ferries, trucking, freight rail, and passenger rail, we work collaboratively with public and private sector partners to develop and to implement programs that promote commerce while enhancing security and mitigating the risk to our nation's transportation systems. We strive to maximize participation from state, local, tribal, and industry interests with a common goal of securing all modes of transportation.

DHS's Mission to Prevent Terrorism and Enhance Security

TSA secures and safeguards mass transit and railroad operations through a variety of programs. Many of these programs enhance security by addressing policy gaps, enhancing coordination, and maximizing the use of partner strengths and capabilities as addressed in the March 2010 Surface Transportation Security Priority Assessment. The primary mission of the Department of Homeland Security (DHS) – Preventing Terrorism and Enhancing Security – is strongly supported by TSA and is aligned with DHS's programmatic activities and organizational structure as found in the 2010 Quadrennial Homeland Security Review and corresponding Bottom-Up Review Report.

Due to the large populations and substantial infrastructure served by mass transit and national railroad systems, these networks remain a target for terrorist groups. Moreover, an open

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00458 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.084

architecture connecting millions of passengers in major metropolitan areas creates inherent potential security vulnerabilities. TSA thus employs advanced risk-based, intelligence-driven techniques to prevent terrorist attacks and to reduce the vulnerability of the nation's transportation systems to terrorism.

Recognizing that the risk from terrorism and other hazards to surface transportation demands a coordinated approach involving all sector partners and stakeholders, the federal government initiated a comprehensive review of U.S. surface transportation security efforts across all modes of surface transportation in 2009. The resulting Surface Transportation Security Priority Assessment (STSPA), released in April 2010, identified interagency priorities for the following four years and provided concrete recommendations on how to enhance security efforts and maximize the use of partnerships to optimize public safety, facilitate commerce, and strengthen the resiliency of the country's surface transportation system.

DHS has completed risk-based implementation plans for each of the 20 consensus recommendations of the STSPA, further addressing the potential risks to the surface transportation system and its four subsectors (mass transit and passenger rail, highways and motor carriers, freight rail, and pipelines). These plans focus on improving information sharing, increasing coordination among federal agencies involved in the transportation sector, and improving the effectiveness and efficiency of the grants process. As of May 2011, 10 recommendations have been fully implemented and the implementation of the others is underway.

Collaboration with Federal, State, Local, Tribal, and Private Entities

Over the past several years, DHS has been working to establish a new architecture in order to better defend against these evolving terrorist threats. This new architecture includes an emphasis on collaboration across government as well as in concert with private industry and the American public.

In 2005, DHS and the Department of Transportation (DOT) signed the Public Transportation Security Annex to the DHS/DOT Memorandum of Understanding (MOU). This agreement promotes security collaboration between federal, state, local, tribal, and private entities. To implement the Annex, TSA – in collaboration with DOT's Federal Transit Administration and the Federal Emergency Management Agency's Grant Programs Directorate – develops a framework to leverage each agency's unique resources and capabilities. The Annex

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00459 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.085

also identifies specific areas of coordination among the parties including citizen awareness, information sharing, security standards, data collection and analysis, and technical resource documents.

In 2010, in collaboration with the U.S. Department of Justice and Amtrak, TSA announced a significant step toward enhancing the security of the nation transportation infrastructure with the implementation of the Nationwide Suspicious Activity Reporting Initiative (NSI) capability throughout the entire Amtrak rail system. The NSI is a partnership among federal, state, and local law enforcement to establish a standard process for law enforcement to identify and report suspicious incidents or activity and share that information nationally so it can be analyzed to identify broader trends. Under this collaborative program, Amtrak officers are also utilizing an upgraded reporting system—made available by TSA —to refer suspicious activity reports to DHS and the Federal Bureau of Investigation (FBI) for analysis and follow-up.

DHS fosters regional security coordination and to integrate the spectrum of available resources for enhanced deterrent and response capabilities while empowering our state and local partners through training and exercise grant programs like the Department's Transit Security Grant Program. TSA works to improve security with security stakeholders outside of the federal government. Key partners include trade groups representing mass transit and passenger railroad interests and the mass transit and passenger railroad agencies as well as senior executives, law enforcement chiefs, and emergency responders. The sector partnership model under the National Infrastructure Protection Plan (NIPP) provides a strong framework for TSA to work with other federal, state, local, and private sector partners on critical infrastructure protection and resilience, especially in the area of surface transportation.

We are also making considerable progress engaging the public in transportation security. DHS launched the "If You See Something, Say Something™" campaign last summer to raise public awareness of indicators of terrorism, crime and other threats, and emphasize the importance of reporting suspicious activity to law enforcement authorities. This campaign is being expanded to places where the NSI is being implemented, to ensure that calls to authorities will be handled appropriately, in an environment where privacy and civil liberties protections are in place. The NSI is currently active in 15 states (California, Florida, Georgia, Indiana, Minnesota, Missouri, Nebraska, New Jersey, New York, Ohio, South Carolina, Tennessee,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00460 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.086

Texas, Virginia, and Wisconsin) and 15 major cities (Boston, Cincinnati, Dallas, District of Columbia, Houston, Kansas City, MO, Las Vegas, Los Angeles, Miami, Milwaukee, Phoenix, Sacramento, San Diego, San Francisco, and Seattle).

To protect the public in this effort, TSA promulgated a final rule that strengthens the process by which individuals can report problems, deficiencies, or vulnerabilities related to transportation security including the security of aviation, commercial motor vehicles, maritime, pipelines, public transportation, and railroad carriers.[1] The rule establishes a mechanism by which an individual who makes such a report to the TSA Contact Center will receive either a written receipt or a call identification number. The receipt mechanism will allow individuals who spot deficiencies in security measures to have documentation in case they receive any retaliation for reporting their coneerns to TSA.

Using Intelligence to Improve Surface Transportation Security

Information sharing is critical to getting resources and intelligence out of Washington, D.C. and into the hands of state and local law enforcement, giving those on the frontlines the tools they need to protect local communities. Timely, accurate intelligence and security information is provided by TSA to mass transit and passenger railroad agency officials through joint efforts among DHS Office of Intelligence and Analysis, TSA Office of Intelligence, and FBI classified intelligence and analysis briefings. Consumers of such information include mass transit and passenger railroad security directors and law enforcement chiefs in major metropolitan areas as well as Amtrak.

Intelligence products are provided to partners through TSA Mass Transit Security Awareness Messages as well as through the Joint Terrorism Task Force network's secure video teleconferencing system. TSA is constantly working with our partners to enhance the scope, accuracy, timeliness, and efficiency of information sharing in order to develop a comprehensive intelligence and security information sharing platform.

Collaborative Risk Assessment Initiatives

TSA is developing and fielding a risk assessment capability focused on individual mass transit and passenger railroad agencies, their regional security partners, and connecting and adjoining transportation systems. This effort aims to produce several risk and vulnerability assessment tools integrated into a single platform so that TSA and its component security

[1] 76 Fed. Reg. 22625 (April 22, 2011).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00461 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.087

partners in DHS can conduct joint assessments of mass transit and passenger railroad agencies, employing resources more efficiently and improving the audit process. In addition, structural vulnerability assessments are currently being conducted on the nation's most critical highway, bridge and tunnel infrastructure. These assessments, performed for TSA by the U.S. Army Corps of Engineers, are the most comprehensive assessments that have ever been performed.

By performing baseline and collaborative risk assessments in the mass transit and passenger railroad domains, TSA is able to engage state and local partners to identify ways to reduce vulnerabilities, assess risk, and improve security efforts. These assessments are conducted with emphasis on the 100 largest mass transit and passenger railroad systems in terms of passenger volume. This group accounts for over 80 percent of all users of public transportation.

TSA uses the Transportation Sector Security Risk Assessment (TSSRA) to evaluate threat, vulnerability, and potential consequences for more than 200 terrorist attack scenarios for mass transit and passenger railroads. TSSRAs rate threat capabilities and likelihood of execution as well as vulnerabilities of rail and bus systems and infrastructure while considering casualties, property damage, and impacts on the transportation network. TSA uses the assessments to inform mitigation priorities, both across the sector and by individual mode, for collaborative security strategies, program development, and resource allocations.

The Baseline Assessment for Security Enhancement (BASE) is a comprehensive security assessment program designed to evaluate 17 security and emergency management action items that form the foundation of an effective security program. BASE is intended to elevate the security posture and readiness throughout the mass transit and passenger railroad network by implementing and sustaining baseline security measures applicable to the operating environment and characteristics of mass transit systems and passenger railroads. TSA implements this continuous improvement process through its Transportation Security Inspectors, who conduct the assessments in partnership with the mass transit and passenger railroad agencies' security chiefs and directors. These evaluations have significantly contributed to an elevation in the mass transit and passenger railroad security posture.

Promoting Surface Transportation Security

In compliance with federal law, TSA has created the Intermodal Security Training and Exercise Program (I-STEP). I-STEP enhances the preparedness of our nation's surface-

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00462 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.088

transportation sector network with meaningful evaluations of prevention, preparedness, and ability to respond to terrorist-related incidents. TSA has assembled a team of federal agencies and commercial vendors to provide planning and strategic support as well as analytical and technical services for transportation security training and exercises under the I-STEP program.

Through outreach, TSA engages all modes of the intermodal transportation community to continuously improve security readiness. I-STEP offers an intermodal transportation-security training and exercise program for our nation's transportation network communities. The program improves the transportation industry's ability to prepare for and respond to a transportation security incident by increasing awareness, improving processes, creating partnerships, and delivering transportation network security training and exercises.

In addition to I-STEP, 25 Visible Intermodal Prevention and Response (VIPR) multi-modal teams are currently being operated by TSA while the FY 2012 budget request includes funding for 12 additional VIPR teams. These teams consist of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to deter potential terrorist acts. Working alongside local law enforcement agencies throughout the transportation domain, TSA's VIPR teams enhance the agency's ability to leverage a variety of resources quickly in order to increase security in any mode of transportation anywhere in the country. TSA conducted more than 8,000 VIPR operations in the past 12 months, including more than 3,700 operations in mass transit and passenger railroad venues. VIPR operational plans are developed with a risk-based methodology in conjunction with local transportation security stakeholders and conducted jointly by TSA, local law enforcement, and transportation security resources.

TSA and the representatives of the Transit Policing and Security Peer Advisory Group work together to enhance coordination and deterrent effects of VIPR team operations. This cooperation has grown since the mutually agreed upon operating guidelines for "Effective Employment of Visible Intermodal Prevention and Response Teams in Mass Transit and Passenger Rail" were implemented in October 2007.

Advancing Security Initiatives through Federal Grants

As I previously mentioned, DHS employs a comprehensive transportation security grant program (TSGP) to provide awards to eligible transit agencies to assist state and local governments in devising and implementing initiatives to improve security. The TSGP promotes

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00463 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.089

a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism. The program is the primary vehicle providing funding assistance for security enhancements to eligible domestic mass transit and passenger railroad agencies and employs risk-based prioritization for funding decisions.

In 2010, the TSGP provided $273.4 million to the transit and passenger railroad industry and a total of $1.6 billion since 2006. Similar, but smaller grant programs have supported over-the-road bus operations. Approximately $175 million has been awarded through TSGP for operational deterrence activities, which include public awareness campaigns, training, drills, and exercises since FY 2006. TSGP funding also supports non-federal law enforcement positions for anti-terrorism activities. DHS has awarded $29.9 million since FY 2006 for 60 canine teams and $93.6 million for 304 officers to create 77 anti-terrorism teams. These officers enhance security, provide a visible deterrent and augment our nimble, risk-based approach to provide assistance where it can best be put to use. Transit, passenger railroad, and law enforcement agencies have also been provided TSGP funds to hire non-federal officers to serve as mobile explosives detection screeners. The officers for each of these teams are employees of the transit system/passenger railroad/law enforcement agency and are deployed according to security needs within the local transit or passenger railroad system.

In an effort to further harden critical surface transportation infrastructure, in 2010, TSA, in coordination with DOT and other DHS offices, developed and implemented the "National Strategy for Highway Bridge Security," to conduct the most comprehensive structural security assessments to date on more than 60 of the nation's most significant highway structures, including bridges, tunnels and terminals. DHS is making strides across the department to improve critical infrastructure protection activities. Grants have been used to support intrusion detection, physical hardening, and surveillance measures for underwater tunnels, bridges, and multi-user high-volume stations. The TSGP has funded $155.2 million for underwater tunnel hardening, $168.5 million for critical station physical security measures, and over $28 million for suspension bridge hardening since FY 2006.

Conclusion

Our goal at all times is to maximize transportation security to stay ahead of the evolving terrorist threat while protecting passengers' privacy and facilitating the flow of legitimate commerce. TSA works collaboratively with industry partners to develop and implement programs that promote commerce while enhancing security and mitigating the risk to our nation's transportation system. I want to thank the Committee for its continued assistance to TSA and for the opportunity to discuss the important issues related to surface transportation security. I am pleased to answer any questions you might have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00464 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.090

STATE OF CONNECTICUT
DEPARTMENT OF
EMERGENCY MANAGEMENT AND HOMELAND SECURITY

TESTIMONY BEFORE SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Peter Boynton, Commissioner
Connecticut Department of Emergency Management and Homeland Security
June 22, 2011

Chairmen Lieberman and Ranking Member Collins, members of the Committee, good morning and thank you for inviting me here today. My name is Peter Boynton and I am the Commissioner of the Connecticut Department of Emergency Management and Homeland Security. Previously, I was the Federal Security Director for TSA at Connecticut's Bradley International Airport, also served as the Coast Guard Captain of the Port in New Haven, Connecticut, and before that, served on the National Security Council staff here in Washington.

First, I want to thank the partners that work together in Connecticut to enhance homeland security, and specifically mass transit security, including the MTA and Amtrak police in Connecticut, TSA, Coast Guard, Connecticut State Police, Connecticut Department of Transportation, the local first responders who patrol and respond to these mass transit corridors every day, DHS for support of, among other things, the Connecticut State Fusion Center, and the importance of continued support from our FBI partners. Thanking our partners includes thanking the public, both the riders and the surrounding residents who are participating in security through a sustained "See Something Say Something" campaign that we launched last fall.

I am here to offer a state perspective on transit security and particularly rail security. There are four themes that I would like to emphasize today: first, the benefit of balancing large city rail security with rail security for the surrounding communities that feed into that same rail system; second, how the evolving terrorist threat drives the need for transit security for both urban areas and the communities which surround them; third, the importance of information sharing and communications in this terrorist threat environment, and; fourth, next steps to enhance the role of the public as a vital partner in rail security.

Connecticut has a mass transit rail system carrying over 127,000 passengers on 289 trains every day. As transit systems go, this is not among the largest, but the notable aspect of the Connecticut transit system is that it is part of the much larger New York City metropolitan area transit system. All of those Connecticut trains and most of the passengers go directly to the heart of New York City – Grand

25 SIGOURNEY STREET, 6TH FLOOR, HARTFORD, CT 06106
AN AFFIRMATIVE ACTION/EQUAL OPPORTUNITY EMPLOYER

67123.092

Central Station. In 2010, there were over 37 million passenger trips from Connecticut into New York City.

The interconnected nature of mass transit means that the security of the New York City transit system relies in part on the security of the Connecticut-based portion of the transit system. Connecticut's situation is not unique. This type of feeder rail system exists elsewhere around the country, where rail lines from surrounding communities meet in the larger urban areas.

From the state perspective, however, we are increasingly seeing federal funding being shifted to large urban areas. This is happening not only with transit security grants, but also through targeted reductions in UASI grants, shifts in port security grants, and homeland security grants.

The focus on security for cities makes sense in many respects, but shrinking security funding for communities with transit links into large urban areas may have the unintended consequence of pushing the risk outside the urban area and increasing the vulnerability for terrorists to prepare outside the city for terrorist activity intended within the city. Connecticut has had real experience within its borders with this phenomenon, including the terrorists involved in the 9/11 attacks and the attempted Times Square bombing – both cases where terrorists intending to attack New York City were in Connecticut.

The challenge is to modify current federal grant criteria to include more proportionate funding for communities surrounding urban areas with connecting transit systems, rather than increasingly focusing transit grants almost exclusively within the city limits for large urban areas. The percentage of the funding needed for those surrounding communities with transit links is not large, but it must be sufficient for those communities to complete basic ongoing security measures already begun such as fencing, lighting, communications, and cameras. Connecticut is unlikely to receive any funding under the new Transit Security Grant Program criteria this year, other than potential additional public awareness funds. While that remains critical, additional funds are needed to complete ongoing security projects. In the last five years, transit security grants have successfully supported work in Connecticut to enhance transit security, with $2 million to $6.3 million per year or 1.5 - 2.5 percent of total transit security grants supporting Connecticut transit security. Although this is a small percentage, it has allowed Connecticut to implement important security enhancements.

In addition to modifying the grant criteria, it may help to use a variation of the Port Security grant model, in which the local Coast Guard Captain of the Port reviews and prioritizes the applications with local port users. In the case of rail security, the local Federal Security Director for TSA might take on a similar role reviewing

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00467 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.093

and ranking transit security grant applications. In this manner, the inter-connected nature of the transit systems can be recognized and grant funding proportionately distributed to avoid the unintended consequence of pushing risk out to surrounding communities.

The need for balancing grant criteria is also linked to the evolving terrorist threat. On the one hand, our federal partners are helping us to better understand the evolution of the terrorist threat. The diversification of the threat requires increased local and community involvement. At the same time, however, the other federal "hand" –the one holding the money—is increasingly shifting federal grant funds to large urban areas at the expense of smaller communities with transit links surrounding large urban areas. As feeder systems to the urban areas, Connecticut and other similar jurisdictions that are part of large metropolitan transit systems need continued federal grant support, not just to protect those within their own borders, but as part of the larger risk mitigation to the entire metropolitan transit system in places like New York City and other cities across the nation.

Balanced grant funding is just one way to achieve increased transit security. Another way is to continue to enhance information sharing between disciplines and across jurisdictions. In Connecticut, for example, we have convened a Transit Security Committee that includes transit agencies such as the Department of Transportation, MTA, Amtrak and State Police as well as representatives from all other modes of transportation, including maritime, aviation, trucking, highway and pipelines. The cross-modal interactions on this committee help to build lines of communication. We have also sought to enhance transit security by increasing the number of TSA transit security operations called VIPRs (Visible Intermodal Protection and Response). These VIPRs are an operational collaboration between TSA, transit police and local, state and federal law enforcement. TSA in Connecticut is among the top five nationally for conducting VIPRs, having increased from 34 VIPR operations in 2009, to an anticipated seven times that number by the end of 2011. Support for these VIPR transit security operations should be increased.

Our focus on enhancing transit security also includes the Connecticut State Fusion Center, where we not only have traditional partners such as DHS, the FBI and State Police, but also, since 2008, a full time TSA transportation security intelligence analyst. Connecticut's fusion center also includes full time local police detectives, which further increases intelligence and information sharing between TSA and other partners by providing access to local police departments, and vice versa. Three recent examples highlight the importance of this relationship. First, TSA identified graffiti that was appearing on aircraft at a number of airports, including Connecticut's Bradley Airport, which is the second largest airport in New England. The information was quickly shared with the state

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00468 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.094

fusion center through our TSA representative. This TSA analyst was also instrumental in sharing and disseminating to transportation partners statewide information learned from a neighboring fusion center regarding the tampering of rails in a local community. The TSA representative in the state fusion center quickly researched and analyzed potential connections to a recent national TSA bulletin. Finally, information on rail gate tampering from another neighboring state fusion center was analyzed and disseminated to local partners through our TSA analyst. Continued support to state fusion centers by TSA and other federal agencies is vital to achieve the level of communication and information sharing and analysis necessary to continue to enhance homeland security for transit and elsewhere.

Another way to enhance security, particularly for open transit systems such as rail lines, is to engage and educate the public. People who commute by surface modes such as rail lines tend to do so every day. These people are the experts on what is "normal" on their everyday route. That's why Connecticut has started a long range, far-reaching "See Something, Say Something" campaign, running for at least a two-year period.

But, as the title of today's hearing reminds us, the next critical step is to "do something." We have made progress towards increasing transit security since 9/11, but as the threat shifts, so must the methods we use to enhance that security. Now we must take it up a notch, to institute a higher level of training and education. The question of what we should "do" should be answered, not just by government policy makers, but by practitioners such as rail conductors, engineers and other employees, first responders such as fire and police, and other members of the rail community including passengers and commercial vendors.

The public use of defibrillators as an emergency medical response tool is an example of how the public can be more fully engaged to "do something." We have moved from a time 30 years ago when CPR training was new and rare to today when defibrillators are installed in many public places, and citizens are trained on how to use them. Similarly, we must move from being aware of security risks, with campaigns like "See Something Say Something", to the next challenge of a more interactive preparedness. Future steps could include, for example, basic emergency response information for commuters and vendors. Moving from CPR to informing the public how to operate defibrillators was a big step towards demonstrating the public's capacity to "do something," and should be a model for what could be done in the homeland security arena such as transit security.

Taking this next step truly exemplifies the spirit of resiliency. Since 9/11, we have improved our ability to withstand and recover, but a key element of resiliency is also the capacity to adapt as the threat shifts. Adding the "do something" concept is an example of adapting. The challenges of security in an open system like rail highlight that security is best when the partnerships are broad and include an engaged and educated public.

Thank you to the Committee for this opportunity to address you, and I would be glad to answer any questions you may have.

67123.095

Center for National Policy

Charting a Secure, Prosperous, and Resilient Future

"Beyond Law Enforcement and Screeners: Elevating the Role of Public Engagement and Resilience in Rail and Transit Security"

Written Testimony to support

a hearing of the

Committee on Homeland Security and Government Affairs
United States Senate

on

"See Something, Say Something, Do Something:
Next Steps for Securing Rail and Transit"

by

Stephen E. Flynn, Ph.D.
President
Center for National Policy
sflynn@centerfornationalpolicy.org

Dirksen Senate Office Building – Room SD-342
Washington, D.C.

9:30 a.m..
June 22, 2011

One Massachusetts Avenue, NW, Suite 333 • Washington, DC 20001 • Phone (202) 682-1800 • Fax (202) 682-1818
E-Mail: info@centerfornationalpolicy.org • Homepage: www.centerfornationalpolicy.org

"Beyond Law Enforcement and Screeners:
The Role of Training and Public Education in Rail and Transit Security"

Dr. Stephen E. Flynn
President, Center for National Policy

Chairman Lieberman, Ranking Member Collins, and distinguished members of the Committee on Homeland Security and Government Affairs. I am honored to have this opportunity to testify on the critically important issue of rail and transit security nearly ten years after the attacks of September 11, 2011.

At the outset, it is important to acknowledge, that rail and transit security simply have not been a priority for the Bush and Obama Administrations, both in terms of policy focus and dollars and cents. By one estimate, typically $9 is spent on security for every passenger who flies. Meanwhile we are spending roughly one penny per rail and transit passenger.[1] When it comes to this critical sector, as a nation we have barely crossed the starting line. But, there is a potential silver lining to the embryonic state of rail and transit security. We can avoid trying to replicate the kind of costly enforcement-centric approach that generally assumes operators and users pose a potential threat to the system unless they are subject to screening by security officials. In its place, we can invest in a more effective, sustainable, and affordable system of reaching out to commuters and workers who operate in and around rail and transit systems, and inform, empower, and support them as part of solution before, during, and immediately after a security incident. We can also assign a higher priority to effectively responding and recovering from intentional attacks and accidental incidents in order to reduce the disruptive appeal of targeting the rail sector.

Assessing the Threat:

The renewed attention to rail security has been animated by intelligence gathered by U.S. Special Forces during their May 1, 2011 raid on the compound of Osama bin Laden that pointed to possible al Qaeda plots to derail trains in the United States. The vulnerability is a real one as confirmed just a few days ago when Amtrak announced that it would be stepping up security along its rail lines while the FBI investigated the discovery on Jun 11, 2011 of an incident of intentional tampering of a switch box along an Amtrak route in Iowa. Post-9/11 terrorist attacks in Madrid, London, and Mumbai also make clear that trains and train stations are in the crosshairs of contemporary terrorist organizations.

The evolution of the terrorist threat in recent years suggests that there is good cause to revisit the state of rail and transit security within the United States. Since 2008, I have been honored to serve as a member of the National Security Preparedness Group (NSPG), led by former 9/11 Commission chairs, Governor Tom Kean and Congressman Lee Hamilton. In September 2010, the NSPG released a report *Assessing the Terrorist Threat,* that found that the United States is facing a growing risk of small-scale attacks executed by homegrown terrorists. A number of recent studies and reports seem to

[1] Testimony from James C. Little, International President of the Transport Workers of America, AFL-CIO, before the House Committee on Homeland Security. February 13, 2007. http://chsdemocrats.house.gov/SiteDocuments/20070213174618-07221.pdf

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00471 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.097

confirm these assessments. In February 2011, the New America Foundation and Syracuse University published a report that found that "nearly half" of the 175 cases of Al Qaeda related homegrown terrorism since September 11, 2001, occurred in 2009 and 2010.[2] Among the most serious incidents, and the one most relevant for the topic of the hearing today, is the September 2009 plan by Najibullah Zazi to blow up the New York City subway.

The fact that trains are receiving more attention by terrorists arises in no small part because passenger aviation has become a much more difficult target to successfully hit. It also is the byproduct of the fact that so much of the al Qaeda's senior leadership infrastructure including the May 1, 2011 death of Osama bin Laden, has reduced the capacity for al Qaeda to plan and execute sophisticated large-scale attacks in North America. Large-scale attacks organized by aligned groups or other terrorist organizations are still possible, but they are increasingly difficult to carry out without attracting attention. This is because catastrophic-scale attacks require a group of operatives with a capable leader, communications with those overseeing the planning, and time to conduct surveillance and rehearse the attack. Money, identity documents, safehouses for operatives, and other logistical needs have to be supported. All this effort ends up creating multiple opportunities for detection and interception by intelligence and law enforcement officials.

But attacks on freight trains and mass transit can be carried out by homegrown operatives, acting as lone wolves or with one or two accomplices. As such, these attacks are far more difficult for the intelligence community to detect and for federal law enforcement to intercept. These smaller-scale attacks can also achieve results similar to large-scale attacks as the attempted bombing of Northwest Airlines Flight Number 563 on Christmas Day 2009 dramatically illustrated. In that case, al Qaeda operatives observed that even a near-miss attack can generate considerable political fallout and a rush to impose expensive and economically disruptive new protective measures. Since relatively small and unsophisticated attacks have the potential to generate such a big-bang for a relatively small investment, the bar can be lowered for recruiting terrorist operatives, including those who belong to the targeted societies.

The October 2010 air cargo incident involving explosives hidden ink cartridges shipped from Yemen is consistent with this trend towards smaller attacks, but with the added element of aspiring to create significant economic disruption. The would-be bombers had no way of knowing that the cartridges would end up on a commercial airliner with hundreds of passengers or a dedicated air cargo carrier with a small crew. That was not important since they understood that destroying any plane in midair would trigger U.S. officials and others to undertake an extremely costly and profoundly disruptive response that would undermine the movement of global air cargo.

---

[2] "Post-9/11 Jihadist Terrorism Cases Involving U.S. Citizens and Residents," *A Study by the New America Foundation and Syracuse University's Maxwell School of Public Policy,* March 2011, available at http://homegrown.newamerica.net/.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00472 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.098

To summarize, in the absence of a new security emphasis on mass transit systems and rail freight, the rail sector is likely to be increasingly targeted by terrorist organization. These systems are relatively easy to access since they provide multiple entry points, very often over a vast geographic area, with little to no physical security barriers to entry. Homegrown terrorists are likely to familiar with these systems. Attacks on mass transit, especially stations, particularly when undertaken during peak-commuting hours, can potentially yield greater loss of life than an attack on a single aircraft. At the same time, should such an attack lead to the shutting down of a transit system or the movement of freight, the resultant denial of service can be crippling to a major urban economy and regional supply chains.

How Not to Advance Rail and Transit Security:

In crafting a way forward in rail and transit security, the federal government should first commit itself to avoiding four-missteps that have marked the post-9/11 approach to homeland security.

First, efforts to bolster rail and transit security *should avoid alienating the very public that security officials are obligated to protect.* The need to focus on maintaining the hearts and minds of the public while providing security is a lesson that was learned the hard way by the U.S. military in Iraq and it is now imbedded in the Army Field Manual that guides counterinsurgency operations. While it is true that the public can generally be compelled to submit to new security measures as a condition of their gaining access to transportation systems, coercing submission to screening and enforcement rules has the downside risk of fueling resentment and undermining the willingness of the public to actively support security efforts. Alternatively, when the general public understands and views an effort to advance security as appropriate, they will actively collaborate in achieving its goal. When it comes to rail and transit security, federal officials should pursue efforts that engender the support and active involvement of the riding public and the operators they serve.

Second, *do not promise more than can be delivered.* No security regime will be fool proof. This is why it is a bad idea for public officials to be tightlipped about the known limits of any specific technology or protocol. The new scanning technology now in use at U.S. airports can be evaded by common drug smuggling techniques. At U.S. seaports, radiation portals have been deployed with considerable fanfare to support the inspection of inbound containers. But these portals are unlikely to detect shielded nuclear material which means that a nuclear weapon or even a dirty bomb encased in lead could pass through the portals without triggering an alarm. Allowing unrealistic expectations to go unchecked guarantees disappointment and mistrust over the long run.

A corollary of this rule is to be wary of measures that are weighted more towards providing the "optics of security" rather than real security. For example, the presence of cement barriers outside a train station may reassure daily commuters. But if those barriers are not anchored to the ground, an explosive-laden truck could ram them aside and make it to the station's entrance. The ensuing tragedy would leave commuters feeling rightfully deceived and the families of victims outraged. Security protocols must

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00473 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.099

survive a "morning-after test"; that is, they should be able to withstand a postmortem by the public about their adequacy, even if they failed to thwart an attack. If the post-incident assessment deems the security measures to be lacking credibility, there will be hell to pay.

Third it is important for federal officials to *resist the secrecy reflex*. Too much homeland security-related work is being done behind closed doors. On its face the oft-stated rationales for this secrecy are compelling. For instance, it seems sensible to avoid identifying vulnerabilities that potential adversaries might then decide to target. Also, if the details of security measures are publicly know, a determined adversary might devise a successful work around. And too much candor about threats and vulnerabilities might generate excessive public fear.

But the proclivity for the national security, intelligence, and federal law enforcement communities to operate in a world of classified documents and windowless rooms is counterproductive. Too often, the people who design, operate, or manage critical systems are left out of the security loop. This is especially the case with critical infrastructure such as mass transit and rail freight systems. As a result, most of the expertise for devising creative, sensible, and sustainable solutions is not being tapped. To determine the best way to protect something like rail freight and mass transit systems, federal officials should err on the side of openness when it comes to sharing information with operators and managers of those systems. Officials should also actively solicit industry input.

While releasing detailed blueprints of protective measures to the general public would be foolish, there is a potential counterterrorism benefit to being more open about what is being done to protect critical systems like rail transportation. This is because the secrecy reflex often ends up working against the goal of keeping public anxiety in check. People are most frightened when they sense they are vulnerable to a threat but feel powerless to deal with it. For nearly a decade Americans have been hearing that terrorism is a clear and present danger. But more often than not, they have been told to go about their daily routines because their government is hard at work protecting them. This is much like a doctor telling a patient that she is suffering from a potential life-threatening illness and then providing only vague information about what can be done about it. No one wants to get disturbing news from their physician, but it becomes much less stressful once they get the details of a prognosis, receive a clear outlay of the available treatments, and are given the opportunity to make decisions or take actions that provide an element of personal control over the outcome. In the same way, the American public will be less fearful and more prepared if they are given the information they will need to better withstand, rapidly recover from and adapt to the next major terrorism attack. It follows that elevating the *risk-literacy* of Americans should be a top homeland security priority.

The fourth and perhaps most important misstep to avoid is *not overreact*. What is fueling the appeal of terrorism as a tactic against the United States is the confidence that terrorists have that Americans will react by embracing draconian measures with little consideration for cost or unintended consequences. Regrettably, since 9/11, this is

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00474 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.100

precisely the kind of response that Washington has been publicly embracing in both word and deed.

The Way Forward – An Emphasis on Engagement, Empowerment and Resilience

A strategic approach to rail and transit security should have three key elements. It should begin with the recognition that commuters and workers in and around the rail and mass transit system should be seen as the frontlines of prevention. Intelligence and law enforcement officials can play an important support role, but it is unrealistic to assign them the dominant role. Transit and rail systems are difficult to protect because they tend to be open to so many users across a wide geographic area and their operations are very time-sensitive. A typical New York City subway station has at least four entrances for passengers and major stations can have more than a dozen. When trains are delay, platforms can quickly become heavily congested. The MetroNorth, Long Island Railroad, the New Jersey Transit and PATH are regional systems that carry daily commuters across city and even state boundaries. Given the small number of tracks available to support their ridership, these trains must abide by a strict schedule to avoid creating cascading delays throughout the system

While on its face, mass transit looks hopelessly difficult to secure, it has a tremendous asset when it comes to detecting a potential security threat—its riders and operators are very familiar with the system and deeply vested in its safety and efficiency. Unlike aviation where passengers typically have only episodic contact with airport terminals, the overwhelming majority of commuters ride trains every day, often at the same time, and frequently sit in the same area. They are both attuned to the normal rhythm of the transit experience, and are perceptive about any changes. Train conductors often know many of their commuters by face if not by name. Engineers, maintenance, and support personnel are intimately familiar with their operational environment. Ticket agents, taxi drivers, vendors, and shoeshine boys have the means to detect aberrant activity in even the most hectic train station. Everyone is inherently vested in making the transit experience a safe and timely one. All should be asked to share in that responsibility and provided with training and education so that they can be empowered to play that role.

While the New York City "See Something, Say Something" campaign is a helpful stepping-off point, its effectiveness depends on the public knowing what they should be looking out for, who they are saying something to, and what they can expect as an outcome. There are lots of opportunities to communicate with the transit public while they are at stations, on platforms, and aboard trains. Every effort should be made to use contact with riders as "teaching moments." Warnings should have meaningful content and there should be guidance that outlines simple tasks for dealing with emergencies. Outreach should be done to major employers who have a large number of commuters to solicit them in supporting more extensive training efforts. Wherever possible, commuters and their employers should also be encouraged to "do something" such as receive Red Cross training and participate in programs modeled on the Metro Citizen Corps established by the Metro Police in Washington, DC.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00475 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.101

Training of the professionals who operate within and around the transit system needs to be substantially stepped-up. The just-released June 14, 2011, GAO report on "Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing" documents the inconsistency and inadequacy of railroad security training programs around the country.[3] Maddeningly, the failure of TSA to issue regulations for these programs as required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* has effectively put rail security training in a deep freeze for over three years. This is because most local jurisdictions have been hesitant to pursue their own effort until direction arrives from Washington. But the answer is not simply for TSA to rush out new regulations developed by its headquarters staff. These regulations need to be developed with input from transit unions and other transportation professionals who understand rail operations and how security can be effectively integrated into those operations without causing adverse unintended consequences.

One model training program that should be rolled out within major rail stations is *Logan Watch*. Logan Watch takes a whole community approach to terminal security at Boston's Logan Airport. Every employee at Logan Airport receives training on identifying and acting on suspicious activity. Receiving this kind of training should be supported and made an annual requirement at all airports and major transportation terminals around the United States.

The second strategic imperative is to insure that security efforts are appropriately balanced across jurisdictions and not simply concentrated, piecemeal fashion, within the jurisdiction of a few major cities. Rail security also should not be treated in isolation since it frequently connects with other modes of transportation including bus service and ferry service for passengers; and trucks, ships, and barges for freight. One model worthy of emulation for dealing with cross-jurisdictional and intermodal issues is Connecticut's Transit Security Committee that includes security officials from the transit agencies operating within the state, as well as representatives from the maritime, aviation, trucking, highway, and pipeline sectors. These Committees should also include transit representatives from adjacent states when that is appropriate as well as senior managers and transit union representatives. As with Area Maritime Security Committees, formally established regional transit security committees could be provided with an opportunity to vet and prioritize federal grant proposals.

A third strategic imperative is to emphasize the *resilience* of transit systems. Specifically, more should be done to make these systems better able to withstand, and to more effectively response and recover to the probability that they may be targeted some day. Focusing on resilience is not an act of resignation and pessimism. Certainly, pragmatism requires an acknowledgement that there is no such thing as fail-safe prevention measures. We should be prepared for when things go wrong. But improving resilience can actually support the prevention goal by creating a deterrent. Since the primary appeal of engaging in acts of terrorism is the harm it will inflict and the

[3] GAO-11-688T Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing, June 14, 2011, http://www.gao.gov/new.items/d11688t.pdf

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00476 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.102

disruption that it will generate, resilient systems make less attractive targets. If a terrorist attack results in a fizzle instead of a big bang, there is little incentive for an adversary to undertake them.

It is important to recall that the July 7, 2005 attacks on the London Underground were met with a swift and effective emergency response. London emergency responders routinely conduct major drills and exercises. Several of the London firefighters involved in the response to the July 2005 suicide bombing attacks had actually recently received training at "Disaster City" at Texas A&M University and publicly attributed their successful response to that training. Had the emergency response been badly managed, it is likely that London commuters would have been more hesitant to re-board trains the morning after the attacks. In short, investing in effective emergency response is indispensible to quickly restoring a targeted transit system, and a demonstrated capacity to rapidly restoring service is key to deterring/preventing an attack on the transit system in the first place. To this end more funding should be provided: (1) to support transit workers and emergency responders from across the United States to attend the Texas Engineering Extension Service (TEEX) program, and (2) to conduct major transit incident training exercises annually.

To conclude, a renewed focus on transit security provides an opportunity to recalibrate our approach to homeland security so that it draws on America's greatest national security asset—our people. Law enforcement and some security technology can be helpful. However, neither will ever be an effectively substitute for a better informed and empowered transit public, a well-trained workforce, and capable emergency responders.

Chairman Lieberman and Senator Collins, I thank you for this opportunity to testify today and look forward to responding to any questions that you might have.

Stephen Flynn is the president of the Center for National Policy and author of "Recalibrating Homeland Security" that appears in the May/Jun 2011 issue of Foreign Affairs.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00477 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.103

THE TERRORIST THREAT TO SURFACE TRANSPORTATION

Brian Michael Jenkins
Director

National Transportation Security Center of Excellence
Mineta Transportation Institute

June 2011

Public surface transportation—trains, buses, stations, even groups of people waiting at bus stops—offers terrorists an attractive target: easy access and easy escape; concentrations of people that enable attackers to achieve high body counts; confined environments that enhance the effects of explosives and unconventional weapons; opportunities to cause great disruption.[1]

The terrorist threat to public surface transportation is real. Since September 11, 2001, terrorists have carried out 75 attacks on airliners and airports worldwide causing 157 deaths. During the same period, terrorists (as of May 22, 2011) carried out 1,804 attacks against bus and train targets, killing more than 3,900 people.

Terrorist attacks on surface transportation have increased in volume and in lethality. While terrorists remain obsessed with attacking aviation targets, the number of terrorist hijackings and sabotage attempts has declined. At the same time, however, terrorist attacks on trains and buses have increased. Counting only incidents with fatalities to avoid increases due solely to better reporting, terrorists carried out a total of just 15 attacks with fatalities between 1970 and 1979. The number grew to 43 attacks with fatalities in the 1980s, 281 in the 1990s, and 465 between 2000 and 2009.

Terrorists see surface transportation as a killing field. Eleven of the attacks since 9/11 resulted in 50 or more deaths and three of the attacks killed nearly 200 people. The total number of fatalities in these 14 attacks is the approximate equivalent of seven airline crashes.

The West is not immune. Most of the attacks and the more lethal attacks have occurred in the developing countries like India and Pakistan, but there have been significant terrorist attacks on trains in Spain, the United Kingdom, Russia and Japan. Further terrorist attacks have failed in the United Kingdom and Germany and serious terrorist plots have been uncovered in several countries.

---

[1] This Testimony draws on research sponsored by the Department of Homeland Security, the Office of University Programs, and the Department of Transportation's Research and Innovative Technology Administration.

67123.104

It can happen here. Since 9/11, there have been seven reported terrorist plots involving attacks on trains in the United States.

The Mineta Transportation Institute's database shows that:

- Bombs were used in 74 percent of all attacks.
- There were more attacks against bus targets than train targets (49 versus 26 percent) but attacks on trains are on average more lethal with 5 fatalities per attack versus 3 fatalities per attack for buses.
- Suicide attacks are less lethal than concealed bombs left behind in passenger compartments, which are the most lethal form of attack. (This has important security consequences.)
- Jihadist terrorist attacks on surface transportation are most lethal. More of their attacks involve fatalities; and nearly nine percent of these involve more than 25 fatalities each.

We should not fixate on suicide bombers. Obviously, not all security measures work against suicide bombers, but recruiting suicide bombers is difficult and significantly raises the threshold for attackers. Only two of all of the jihadist terrorist plots in the United States involved suicide attacks. And the deadliest terrorist attacks on trains in Madrid and Mumbai involved bombs concealed in abandoned backpacks and suitcases.

Employee and passenger awareness counts: 16 percent of bomb attacks have been stopped prior to their detonation because of an aware public. More can be done here.

HIGH-SPEED RAIL – TOMORROW'S TERRORIST TARGET?

Terrorist attacks on high-speed rail systems have occurred in France, Germany, Japan, Russia, Spain and Switzerland. In Europe, Asia and North America, high-speed rail trains are seen as icons of a country's identity and economic power, and typically they serve a customer base that represents the country's government and business elite.

When terrorists attack high-speed rail systems, they seem to prefer to derail trains. When they go after non-high-speed rail systems, they more often try to detonate bombs in passenger compartment. Most attacks on high-speed rail systems target the tracks (66 percent) versus the passenger compartment (17 percent). More attacks on non-high-speed rail systems target the passenger compartment than the tracks.

Terrorists choose between volume and velocity. Passenger loads on high-speed rail trains, per-car and per-train are less than slower-speed commuter or regional trains. This explains why high lethality with bombs detonated in passenger compartments is more achievable on a non-high-speed train. On the other hand,

67123.105

train velocity is obviously much greater on high-speed trains, making collisions or derailments a more attractive and effective choice of attack method.

Was Osama bin Laden on the right track? Based on a statistical review of outcomes from accidents on high-speed rail systems, the ultimate tactical goal for terrorists most likely would be to focus on a derailment that forces the train to either collide at high speed with another train, bridge abutment or wall, or go off a bridge or embankment into a body of water or fall/roll down a significant elevation.

Bombs placed on the tracks are on average twice as lethal for high-speed rail than those placed in the passenger compartments. For non-high-speed rail, bombs in passenger compartments have proved to be more lethal than bombs on the tracks.

Overall, derailments involving mechanical means of sabotage have proved that they can be more lethal than bombs on the tracks. Technology, particularly on high-speed rail systems, will cause train operations to cease if a bomb detonates and causes catastrophic destruction prior to train arrival. Effective use of explosives, as in the Russian Nevsky Express attack in 2009, requires the detonation to be timed perfectly with a train's passage. Even in this attack, more casualties were crush and impact injuries and fatalities, occurring in the derailing rear cars (numbers 12, 13, and 14) of the train than those caused by the explosion under the 9th car.

High-speed rail track and equipment safety enhancements have made accidental derailments less lethal. High-speed trainsets are designed with relatively rigid, semi-permanent connections while slower-speed trains rely on traditional "knuckle" couplers. These more rigid connections greatly reduce the probability of a train "jackknifing," or of partially or completely rolling over. Non-high-speed passenger trains tend to jackknife or flip over, causing a significantly high number of injuries and fatalities. Track designs have incorporated enhancements to guide and guard rails which keep a derailed train moving upright, along the right of way, keeping it from going off bridges, down hills, and away from trains on other tracks or bridge abutments and walls. Brackets have been added to high-speed train wheel sets in Japan to keep a derailed train on the track, reducing the probability significant casualties in an accidental or intentional derailment.

Causing a derailment and/or collision by compromising the track structure or signal system might be an effective attack to execute. This could be done through mechanical sabotage or cyber attacks on the controlling computer systems.

The most catastrophic accident outcomes have been due to higher speed (80 to 100mph+) collisions with other trains or fixed objects. While it hasn't been used as an attack method to date, moving a locomotive or a string of cars into the path

67123.106

of an oncoming high-speed train is a tactic that should be considered and prevented. In the 2010 derailment of the Bengal Express, which killed 148 people, moments after the passenger train derailed, a freight train going in the opposite direction plowed into the derailed passenger coaches. It is not certain if the saboteurs intended this to happen.

A REALISTIC APPROACH

With federal assistance, transportation security clearly has improved during the last ten years. More can be done, of course, but security proposals must be realistic.

Security for surface transportation must comprise the entire spectrum of measures from deterrence and detection to mitigation and emergency response. Aviation security is "front-loaded," that is, it aims at prevention. There are few opportunities to save lives after a plane crashes. Surface transportation security cannot be front-loaded, but there is much that can be done to mitigate casualties and to save lives after an attack, as well as minimizing damage and expediting recovery process.

Protecting public places that, by their very nature, require easy access is difficult and costly. To be worthwhile, security must provide a net security benefit. The result cannot be a mere diversion of the attack to another accessible public place where the attacker can achieve the same results in casualties.

Security must take into account economic realities. Federal resources will be limited. Many local governments are broke. Transportation systems' operators are hard pressed to keep costs down. We need not just more, but smarter security. We need low-cost solutions.

Security must be sustainable. We cannot look forward to the end of terrorism when the security structures erected over the past several decades can be dismantled. Security measures put into place today are likely to become a permanent feature of the landscape. Therefore, they must be sustainable in terms of public acceptance, disruption, and costs for operation, maintenance, upgrades, evaluation, and replacement.

The aviation security model will not work for surface transportation. Surface transportation systems are too diverse. Screening of all passengers would be nearly impossible. Train stations have too many access points. The volumes of passengers are too great. The number of screeners required would run to the hundreds of thousands. The costs would be prohibitive, the delays intolerable.

There is no near-term technological solution. New explosives detection technologies are being developed, but their probability of detection with acceptable false alarm and throughput rates in a real operating environment are

67123.107

not clear. In addition, their deployment will require thorough application evaluation, new policies, and training. What do we do when "Stand-off" detection identifies a possible suicide bomber in a corridor packed with passengers?

Americans must be realistic about security. One hundred percent security in surface transportation is not possible. Some risk is unavoidable, just as when we drive our automobiles, but the risk to individual citizens from terrorism is minuscule.

SOME EASY GAINS

The role of the federal government will be to lead in research, develop and test new security technology, evaluate security policies and practices, disseminate information pertaining to the threat and best security practices, and assist local governments in acquisition and training. Canines specifically trained in explosive vapor wake detection are a new and important development.

More resources are required at the local level for security enhancements and training. In today's environment, these will necessarily be limited.

Initial and ongoing security training is required for frontline transportation employees—train drivers, conductors, station personnel, not just managers, as well as emergency responders. But providing it raises cost and logistical issues.

Passengers can be enlisted as partners in their own security. Current "see something, say something" campaigns are a first step. They need to be evaluated to see if the message is getting through and how better to engage the public. Communications have to be facilitated. Procedures have to be established to ensure rapid diagnosis and response. Callers need to be acknowledged, for their efforts, even when it turns out to be a false alarm. Disruptions must be minimized.

Synergies between safety and security measures as well as between crime prevention and counter-terrorism efforts need to be identified and exploited to increase efficiencies in resource deployment and allocation.

67123.108

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Mary L. Landrieu

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 23, 2011

Question#:	1
Topic:	IED
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: The Department of Homeland Security's Science and Technology Directorate is working with TSA on a number of research projects related to rail and transit security. One of these initiatives is focused on domestic IED detection. Please share your views on the IED threat to rail and transit systems within the United States, the status of technology development within the Department to address this threat, and the potential impact that House-proposed cuts to the Department's Science & Technology budget could have on these efforts.

Response: TSA considers the Improvised Explosive Device (IED) a serious threat to rail and transit security, given the potential consequences of such an attack. The Department of Homeland Security's Science and Technology Directorate (S&T) and TSA collaborate on a range of security technologies to address the unique capability gaps and vulnerabilities associated with mass transit systems. These technologies include those that address person-borne IEDs, leave behind package screening, vehicle-borne IEDs, intrusion detection, and infrastructure protection. In support of layered security and risk-based concepts, technologies are being developed and assessed through testing and field pilots. The House-proposed cuts to S&T's Fiscal Year 2012 budget would delay the development and testing of technologies for mass transit security.

67123.109

Question#:	2
Topic:	VIPR
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide some additional information on the VIPR teams currently operating around the United States, the 3,700 operations they conducted in mass transit and passenger railroad venues over the last 12 months, and the deployment plan for the 12 new teams proposed in President's FY12 budget request.

Response: Visible Intermodal Prevention and Response (VIPR) resources, comprised of Transportation Security Administration(TSA) Office of Security Operations and Office of Law Enforcement/ Federal Air Marshal Service assets, are deployed throughout the nation. With the FY 2010 budget enhancement, VIPR teams are now based in 25 locations: Atlanta, Boston, Charlotte, Chicago, Cincinnati, Cleveland, Dallas, Denver, Detroit, Houston, Las Vegas, Los Angeles, Miami, Minneapolis, New York, Newark, Orlando, Philadelphia, Phoenix, Pittsburgh, San Diego, San Francisco, Seattle, Tampa and Washington, D.C. These teams provide a nationwide footprint in response to risk-based needs.

VIPR teams can include Federal Air Marshals, Behavior Detection Officers, Transportation Security Inspectors, Transportation Security Specialists – Explosives, Explosives Detection Canine Teams, and Transportation Security Officers. These TSA resources deploy with other federal, state and local law enforcement and transportation security resources to augment security in every mode of transportation. Deployments are risk-based.

During the past 12 months, VIPR operations have been conducted at mass transit locations in approximately 350 cities across the Nation. In this time, TSA conducted more than 3,700 operations in mass transit and passenger railroad venues. TSA's Transportation Sector Security Risk Assessment (TSSRA) provides modal guidance. The subject matter experts in TSA's Office of Transportation Sector Network Management (TSNM) conducted a risk-based assessment of the infrastructure of each mode and created corresponding high risk lists. The VIPR program has provided this information to the VIPR contacts in each area of responsibility (AOR) to provide input for stakeholder relationship building and deployment planning.

The appropriation request for twelve additional teams in FY 2012 would increase the capacity of the VIPR program to deploy to more locations and to support transportation concerns for national security events. Based on the risk-based assessment process, the VIPR program currently proposes to deploy two additional teams each to be based in Los Angeles and the National Capitol Region and one additional team each to be based in Baltimore, Boston, Chicago, Houston, New York, Newark, Seattle, and San Francisco.

67123.110

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Susan M. Collins

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 23, 2011

Question#:	3
Topic:	governments
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: How would you characterize the cooperation between federal, state, and local governments and the private sector in rail and surface transportation?

Response: The Transportation Security Administration (TSA) enjoys robust cooperation between federal, state, and local governments and the private sector in rail and surface transportation. TSA pursues continuous engagement with stakeholders at all levels to foster regional security coordination, and uses available resources to foster enhanced deterrence and response capabilities. A close partnership between TSA and its stakeholders is integral to TSA's continuing strategic goal of enhancing the security of mass transit and passenger rail.

67123.111

Question#:	4
Topic:	support
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Can you explain TSA's current support for the "See something, Say something" campaign? How much additional support do you anticipate giving, and what is the time frame for implementing the campaign in critical regions?

Response: The trademarked name of the initiative, "If You See Something, Say Something ™" campaign, is being run out of the U.S. Department of Homeland Security's (DHS) Headquarters at the direction of Secretary Napolitano. The initiative, originally used by the New York Metropolitan Transportation Authority (MTA), was licensed to DHS to engage the public to raise public awareness of indicators of terrorism and crime, and emphasize the importance of reporting suspicious activity to law enforcement authorities.

The campaign utilizes existing Department resources for its partnerships and TSA plays an important role in the initiative. In addition to designing all of the graphics/materials, such as posters or images for electronic media for the "If You See Something, Say Something ™" public awareness initiative, TSA also supports the "If You See something, Say Something ™" initiative through the Transit Security Grant Program (TSGP).

Since FY 2006, through TSGP, DHS has funded almost $46M in public awareness campaigns, including "If You See Something, Say Something ™" to high risk mass transit and passenger rail agencies in critical regions. Currently, several mass transit and passenger rail systems that are TSGP grant recipients have implemented, or are in the process of implementing, the campaign. These systems include the New York Metropolitan Transportation Authority (MTA), Washington Metropolitan Area Transit Authority (WMATA), New Jersey Transit, and Massachusetts Bay Transportation Authority (MBTA). The initiative is being launched in conjunction with the Nationwide Suspicious Activity Reporting Initiative (NSI), which is run by the U.S. Department of Justice. As locations become part of the NSI, the "If You See Something, Say Something ™" campaign is rolled out at those locations. TSA intends to continue its support for this campaign and anticipates that it will continue to expand in critical regions.

67123.112

Question#:	5
Topic:	update
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Can you to give us an update on the implementation of 20 recommendations from the Surface Transportation Security Priority Assessment; what the timeline is for implementation is and how far along we have come in implementing them.

Response: The Department of Homeland Security has completed risk-based implementation plans for each of the 20 consensus recommendations of the Surface Transportation Security Priority Assessment, addressing the potential risks to the surface transportation system and its four subsectors (mass transit and passenger rail, highways and motor carriers, freight rail, and pipelines). These plans focus on enhancing information sharing, increasing coordination among federal agencies involved in the transportation sector, and improving the effectiveness and efficiency of the grants process. The timelines to implement these recommendations vary in length; some are already completed and others extend into Fiscal Year 2014. As of July 2011, 10 recommendations have been fully implemented, and implementation of the others is underway.

67123.113

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Joseph I. Lieberman

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 23, 2011

Question#:	6
Topic:	I-STEP
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: TSA's Intermodal Security Training and Exercise Program (I-STEP) has only conducted four exercises nationwide in the last fiscal year and plans to conduct 10 exercises this year. What has prevented TSA from implementing I-STEP more widely before this year? Do you expect to continue to expand I-STEP?

Response: The Transportation Security Administration's (TSA) Intermodal Security Training and Exercise Program (I-STEP) completed 29 exercises nationwide in Fiscal Year (FY) 2010 in support of the requirements of the "Implementing Recommendations of the 9/11 Commission Act of 2007". In FY 2011, I-STEP has already completed 17 exercises, and plans to complete an additional five exercises by 30 September 2011, as a means of building and sustaining security preparedness to protect the American people, enhance national resilience, and identify capability gaps and resource needs. Looking forward, the I-STEP program plans to conduct 20 to 25 I-STEP exercises annually with transportation security and industry partners. Additionally, TSA is expanding exercise planning capacity by introducing an on-line exercise planning and information management system (EXIS), supporting all modes in the transportation system.

Question#:	7
Topic:	TSA
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Dr. Flynn has stated that TSA should do more to enhance resiliency in the rail and transit sector given the difficulties of preventing an attack in a very open environment. Yet TSA's budget for surface security is mostly dedicated to prevention techniques. What do you think the balance should be between TSA's prevention efforts and TSA's efforts to strengthen the resiliency of transportation networks?

Response: The Transportation Security Administration (TSA) is confident that it has achieved the proper balance of resources between prevention and resiliency in rail and transit. The network of tracks that allows trains to move across the country is vast, complex, and interconnected. No single freight line or single point location disruption would significantly debilitate the transportation of commerce by rail. The railroad's ability to continue operations during Hurricane Katrina and, most recently, the Mississippi River floods demonstrates the resilience of the system. Resiliency for transit systems often comes in the form of alternative transportation. Most of the larger transit agencies have both rail and bus components. If there is a disruption in one of the components that would debilitate transportation in a significant way, the other network component is used to provide the resiliency until both components are back on line.

67123.115

Question#:	8
Topic:	strategy
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Although the national strategy for public transportation security developed by TSA and required by section 1401 of the Implementing Recommendations of the 9/11 Commission Act of 2007 indicated that TSA would issue regulations governing transit security, few such regulations have in fact been promulgated. As a result, Surface Transportation Security Inspectors (STSI) have few consistent, defined standards against which to conduct their inspections. Instead, they are generally left to resort to using transit agencies' own voluntarily developed security plans as the standard to measure against.

What can be done to ensure that STSI are conducting adequate and effective inspections and that we are effectively utilizing STSIs?

Currently, inspectors spend more than 50% of their time on freight assessments. When will inspectors be able to conduct inspections, and not simply assessments, for passenger rail and mass transit? Are we currently utilizing STSIs appropriately?

Response: Transportation Security Inspectors-Surface (TSIs-S) must complete an On-the-Job Training checklist and Quality Control Evaluation to ensure standardization and consistency in their inspection and assessment duties across the Nation. Additionally, inspection reports and associated paperwork undergo a review at the local level, prior to being approved, as well as an oversight review by the Regional Security Inspector-Surface. Deficiencies are noted and addressed, as appropriate. Technical training is conducted on an as-needed basis when new inspection types or methodologies are released to the field for action.

The TSIs-S are being utilized to conduct a number of activities in the surface transportation modes including regulatory inspections of freight railroads and rail transit and passenger rail agencies and assessments of mass transit security baseline. While regulations serve an important purpose for compliance, there are many valuable assessments that take place in both the passenger and freight rail communities. In order for transit agencies to be eligible for the Fiscal Year 2011 Transit Security Grant Program, they must have either undergone a security assessment conducted by the Department of Homeland Security, such as the Baseline Assessment and Security Enhancement performed by TSIs-S, or they must have developed or updated their security plan within the last three years.

TSIs-S already conduct inspections to verify compliance with the rail transportation security requirements in 49 CFR Part 1580, and will conduct regulatory compliance inspections of passenger railroads and public transportation agencies after TSA publishes final rules that require security training and vulnerability assessments and security plans.

67123.116

Question#:	9
Topic:	guidance
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In the FY2011 guidance for the Transit Security Grant Program, priority for grants is given to protecting certain specific assets and infrastructure – those on the so-called "top-transit asset list," including certain bridges, tunnels, etc. – rather than to projects that protect passengers and the systems as a whole from attack, such as closed circuit cameras and other measures designed to prevent explosive devices from being brought onto a train, projects which are assigned the lowest priority. Yet previous attacks on transit systems elsewhere in the world, including London and Madrid, have involved explosives carried onto trains, and intelligence analyses, including those from TSA's own Office of Intelligence and from the National Counterterrorism Center, indicate that terrorists would likely target a rail or transit system with multiple, small IEDs in order to cause panic and casualties.

In light of this evidence, and experience, of the nature of the threat against transit systems and their passengers, why, has TSA revised its criteria for grant funding to prioritize funding for a limited number of assets and infrastructure, rather than on protecting passengers and preventing explosive devices, or even chemical or biological agents, from being introduced into the transit system?

For transit systems that cross jurisdictional (including state) boundaries, one side effect of focusing grants on individual pieces of infrastructure, rather than protecting against the introduction of explosives or biological or chemical agents into the transit system on the whole is that funding will likely go to projects sponsored by the individual jurisdictions that own those assets rather than to system wide projects that require the cooperation of the various jurisdictions that comprise the system. In light of this change in funding, and associated incentives, what steps does TSA intend to take to ensure and strengthen regional cooperation?

Response: The Fiscal Year (FY) 2011 Transit Security Grant Program (TSGP) Grant Guidance prioritized projects based on their effectiveness in reducing risk, and maintained the same priority structure and project eligibility in FY 2011 as in FY 2010. The top funding priorities were, and continue to be, operational activities, such as training, drills and exercises, public awareness campaigns, security planning, mobile screening teams, anti-terrorism teams, and canine teams. These operational activities are key elements to the prevention of all types of attacks (including those involving explosive devices and chemical/biological agents), and protecting passengers, by creating an

67123.117

Question#:	9
Topic:	guidance
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

unpredictable deterrence factor, and by engaging transit system employees and riders to become a part of the solution through targeted training and public awareness efforts.

Directing funding towards key infrastructure assets is not new. Funding for key high-density, multi-modal infrastructure, such as underwater tunnels, large stations, and critical bridges, has always been a top priority of the TSGP. Through the introduction of the Top Transit Asset List (TTAL), the Transportation Security Administration (TSA) seeks to focus its limited capital security funding on those surface transportation assets that the Department of Homeland Security considers to be nationally critical in order to completely remediate large assets and show measurable progress in reducing risk.

TSA recognizes the value and successes of regional collaboration and the Regional Transit Security Working Group (RTSWG) process in promoting coordination and collaboration among transit agencies and the Federal government. Independent of the availability of future grant funding, TSA will continue to encourage security-focused coordination and collaboration within regions, including the eight highest risk regions. TSA will work to ensure RTSWGs are security-focused rather than grants/fiscally-focused.

67123.118

Question#:	10
Topic:	risk
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Risk is a complex concept to quantify, but true assessments must evaluate threat, vulnerability and consequence. TSA has indicated that the values assigned to the factors it considers for threat, vulnerability and consequence are generally constant from system to system, and that the only variable in calculating the risk of a system is the number of riders. This seems like an overly simplistic view of risk of any given system. When do you anticipate that TSA will develop and use a more sophisticated assessment of risk?

Response: Regarding threat, an assumption was made that terrorists intend to target transit systems that have a higher ridership and that current tactical methods exist, as demonstrated in attacks in other countries, to execute attacks in these systems within the United States. The terrorists' intent is also assumed to be focused on these systems because higher ridership would most likely result in more deaths and injuries than a system with low ridership. These assumptions about intent and capabilities lead us to conclude that terrorist threats for transit systems with high ridership in high threat urban areas are greater than those with less ridership or in areas not classified as high threat areas.

Regarding vulnerability, transit systems with higher ridership are vulnerable in a number of ways: the volume of individuals requires new, much larger entry and exit points that could be exploited, while providing greater camouflage to conceal a potential bad actor. Also, higher ridership transit systems are more complex, often with multi-level above and below ground terminals and routes, and additional above ground facilities. This complexity means that one attack could affect a terminal that connects more than one, or even many, route(s), thus making the concomitant mitigation efforts more difficult.

Regarding consequence, the contribution of both direct and indirect costs have been considered in the current methodology. Initial analyses suggest that the indirect costs, though difficult to valuate, are relatively constant from one high threat urban area to another. The analyses of direct costs also suggest that physical system impacts and collateral damage are largely constant in the systems considered. Therefore, the most important variable in the consequence determination is ridership—the higher number of individuals killed or injured, the greater the consequence valuation.

While ridership is an important factor in the risk equation, it is not the only variable, however. The risk model also considers underground track miles and infrastructure, and the length and conditions of underwater tunnels. Specifically, as underwater tunnels are remediated, the number assigned to that variable in the model changes to reflect actual vulnerability, and how that vulnerability changes as assets are hardened.

67123.119

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Claire McCaskill

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 23, 2011

Question#:	11
Topic:	reports
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Reports have surfaced that an attack on our rail sector is possible near the anniversary of 9/11. Some analysts have concluded these attacks would be carried out in a coordinated fashion by multiple operatives against several targets.

The TSA is performing "baseline and collaborative" risk assessments for mass transit and passenger rail. Can you explain the difference(s) between baseline and collaborative risk assessments? Are these risk assessments different than the Baseline Assessment for Security Enhancement (BASE) program? If so, how? What funding mechanism is used to create and perform these assessments-- TSA's budget or DHS' transit security grant program?

What type of risk assessments are performed for passenger rail systems located in rural, less densely populated areas? If not being performed, why? Freight rail security is another concern. Kansas City and St. Louis are the number two and three freight rail corridors in the country. How are freight rail security vulnerabilities assessed?

Unlike airports, rail travel is unencumbered by body scans and pat downs. What security assets are provided to state, local and private stakeholders that are not visible to the public? Would some type of proactive action by law enforcement be an effective preventive measure due to its visual nature? If so, does TSA have plans to implement such a program?

Do you believe that some proactive action by law enforcement is more effective security due to the visual aspect? Are there any plans to introduce more stringent security requirements for rail passengers? If so, when?

Response: The Transportation Security Administration's (TSA) budget funds Baseline Assessment for Security Enhancement (BASE). BASE, a comprehensive security

67123.120

Question#:	11
Topic:	reports
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

assessment program designed to evaluate 17 Security and Emergency Management Action Items that form the foundation of an effective security program, is intended to elevate the security posture and readiness throughout the mass transit and passenger rail modes by implementing and sustaining baseline security measures applicable to the operating environment and characteristics of mass transit and passenger rail systems. Through the BASE program, TSA reviews security-related proposals jointly developed by TSA, the Department of Transportation's Federal Transit Administration (FTA), and sector partners from mass transit and passenger rail systems. TSA does not conduct separate collaborative assessments.

The assessment results provide critical data about security priorities, the development of security enhancement programs, the allocation of resources (including security grants), and a compilation of the most effective security practices for mass transit and passenger rail agencies. Over 170 mass transit/passenger rail agencies have participated in a BASE assessment.

TSA uses a risk-based approach when allocating resources. The TSA Transportation Security Inspectors - Surface (TSsI–S) focus the majority of their time on conducting security assessments on high-risk public transportation agencies. Section 1405(b)(1)(A) of the 9/11 Act (P.L. 110-53) requires TSA to conduct security assessments, based on a representative sample, to determine the specific needs of local bus-only public transportation systems. TSA has completed security assessments under the BASE program of 60 bus-only systems, with several in smaller rural areas. TSA has also conducted 19 BASE assessments on passenger rail systems that are not in the high-risk group. These passenger rail systems have for the most part been in mid-size cities, but none of these systems are located in rural, less densely populated areas. TSA has not performed security assessments for passenger rail systems located in rural, less densely populated areas because assessments of those systems are considered a less-efficient use of resources based on TSA's risk model.

Kansas City, Missouri (MO) and St. Louis, MO are recognized as High Threat Urban Areas (HTUA) for the purpose of freight rail security. TSA has evaluated the freight rail operations in both of these areas, and the handling of rail security-sensitive materials is assessed and critical control points are identified. Railroad operators participate in these assessments and are provided with options for consideration to mitigate vulnerabilities. Key railroad bridges in both Kansas City, MO and St. Louis, MO have also been assessed to determine their criticality, and to identify points of vulnerability. The bridge owners participate in these assessments and are provided with a set of options to reduce identified vulnerabilities.

67123.121

Question#:	11
Topic:	reports
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

It is commonly accepted in law enforcement that a proactive visible law enforcement or security presence may reduce the intent and opportunity for a terrorist to operate. Unpredictable presence of security and law enforcement personnel enhances the risk mitigation effects against both planning and conducting terrorist acts.

Another example of proactive visible action of law enforcement is the Regional Alliance Including Local, State, and Federal Efforts (RAILSAFE) program. The primary goal of Operation RAILSAFE is to coordinate deployments of law enforcement personnel from those agencies that could be called upon to help secure the rail system during an emergency or heightened alert.

Question#:	12
Topic:	budget
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The Homeland Security budget which has been received from the House of Representatives has cut DHS' transit security grant program, the funding mechanism for state and local authorities' transit and rail security programs, by over 60%. While this budget is not final our country's fiscal crisis will require budget cuts.

Explain the effects budget cuts will have on present and future rail security programs? What are TSA's plans for streamlining transit and passenger rail security in anticipation of budget cuts?

Response: A reduction in funding will impact the Transportation Security Administration's ability to support future state and local rail security programs, conduct operational deterrence activities, and remediate critical transit infrastructure.

Since Fiscal Year (FY) 2006, the Transit Security Grant Program has funded over $44.1 million for public awareness, and over $131 million for training, drills and exercises. These funding packages have been successful in building in-house transit law enforcement and anti-terrorism capabilities, and have provided just over $157 million for 435 officers for Canine, Mobile Screening, and Anti-Terrorism Teams. Grants have also funded over $350 million, since FY 2006, in critical transit infrastructure hardening and protection actions, including intrusion detection, physical hardening, and surveillance measures for underwater tunnels, bridges, and multi-user, high-volume stations. With the introduction of the Top Transit Asset List in FY 2011, DHS expects to focus funding on complete remediation of nationally critical surface transportation assets. A reduction in funding would affect the future progress of these security efforts.

Currently there is a cap of 10% for grant-funded operational activities. In 2011 this amounts to approximately $20 M and includes training, operational deterrence, public awareness, and drills and exercises. Cuts in the TSGP budget will reduce funding opportunities for these activities proportionately.

Capital expenditures for improving security will also be reduced. Should the funding decrease, remediation of these assets will take longer.

Question#:	13
Topic:	campaign
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony, you stated the "If You See Something, Say Something" campaign is being expanded to raise public awareness of indicators of terrorism.

Explain how the public is trained on the indicators of terrorism? Are there any performance measures in place to rate the effectiveness of this program? If not, why? You explained that using the public is a force multiplier-- more bang for the taxpayers buck. What was the initial start up cost of the program? How much will the expansion of the program cost TSA?

Response: The "If You See Something, Say Something ™" public awareness and engagement initiative is being run out of the U.S. Department of Homeland Security's (DHS) Headquarters at the direction of Secretary Janet Napolitano. The Secretary emphasizes that homeland security begins with hometown security. The goal of the "If You See Something, Say Something ™" campaign is to raise public awareness of indicators of terrorism and crime, and emphasize the importance of reporting suspicious activity to law enforcement authorities to keep our hometowns and our country safe and secure. The public is educated on the indicators of terrorism and crime through a variety of ways. First, when the Department partners with a state, city, sports league or other private sector entity, materials such as posters or electronic images are designed to alert the public what types of things to keep an eye out for and how to report something if they see something suspicious. Also, there is a 10-minute training video that is available on the www.dhs.gov Web site and also has been made available to groups across the country. The Department is continuing to work on materials that can help educate the public.

The Department used existing resources to kick off the campaign. TSA provides support to the campaign by having one of its graphic designers design all of the materials that are used for the campaign – every time DHS launches the campaign with another partner TSA's graphic designer designs all of the materials used – posters, digital/electronic images, etc. Recipients of Transit Security Grant Program (TSGP) grants can use those funds for public awareness campaigns, including "If You See Something, Say Something ™" campaign materials.

Question#:	14
Topic:	rulemaking
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Rulemaking is at the heart of many mandated projects. TSA has yet to fulfill a 2007 legislative mandate requiring uniform transit training programs. Why? The review process should not take four years.

Response: The Transportation Security Administration's (TSA) Security Training Programs for Surface Mode Employees Notice of Proposed Rulemaking (NPRM) is currently being reviewed within the Department of Homeland Security (DHS). Once DHS clears the NPRM, it will be forwarded to the Office of Management and Budget for their review prior to publication in the Federal Register.

Every large, significant rulemaking is a complex undertaking and involves procedural and analytical requirements articulated in a number of Acts and Executive Orders. These laws and orders assure that the necessary analysis and transparency are a systematic part of the regulatory process.

Following a risk-based approach to rulemaking, TSA needed to identify the security gaps; the content and employee coverage of existing training programs; and the relevant entities and employee populations to be covered. Also, the business processes necessary to implement the rule took significantly more time than originally anticipated due to the need to assure that the private sector impact were minimized as much as possible. Another challenge was to ensure that as part of the regulatory design, TSA established a set of processes and procedures consistent across the surface modes targeted by the 9/11 Act, as the requirements for training in the 9/11 Act were essentially the same across the surface modes. See 49 USC 114; Public Law 110-53, section 1408, Public Transportation; 49 USC 114; Public Law 110-53, section 1517, Freight Rail and; 49 USC 114; Public Law 110-53, section 1534, Over-the-Road Buses.

67123.125

Question#:	15
Topic:	genesis
Hearing:	See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Information sharing is the genesis of an intelligence-driven agency. State and local authorities need access to classified information in order to protect life and property from a terrorist attack. If relevant intelligence information is deemed classified by TSA, how do stakeholders access this intelligence?

Response: The Transportation Security Administration (TSA) does not originate classified intelligence; however, TSA works closely with Federal agencies that originate classified intelligence information to disseminate classified and unclassified information to State, Local, Tribal and Private Sector (SLTPS) stakeholders.

SLTPS stakeholders who have proper security clearances can receive classified information through agencies, organizations and partnerships designed for this type of information sharing. Examples include the DHS Office of Intelligence and Analysis, National Counterterrorism Center (NCTC), Joint Terrorism Task Forces (JTTFs) and Fusion Centers. There are also technologies available, such as the Secret Internet Protocol Router Network (SIPRNet) and the Homeland Secure Data Network (HSDN) to disseminate the classified information.

TSA also works with originating agencies to create tear-lines for SLTPS customers who do not have clearances. These tear-lines may contain information on tactics, techniques and procedures of a terrorist group or indications of a potential terrorist attack. Controlled Unclassified Information (CUI) is available through multiple websites, such as the Homeland Security Information Network (HSIN), Law Enforcement Online (Leo.gov) and the Open Source Center.

Finally, SLTPS stakeholders can request clearances through the Department of Homeland security (DHS) or the Federal Bureau of Investigation (FBI).

67123.126

Post Hearing Question and Response for the Record
Submitted to and Answered by the Honorable Peter J. Boynton
From Senator Joseph I. Lieberman

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 22, 2011
Response submitted July 21, 2011

1. According to TSA, the Transit Security Grant Program is its most important tool for securing rail and transit assets.

   - How has TSGP improved security on Connecticut's rail lines? What would be the impact if less funding or no funding was provided from the federal government?

     RESPONSE: Although Connecticut transit is much smaller than New York City transit, 37 million passengers annually go from Connecticut to New York City's Grand Central Station on 287 daily trains. The fact that the TSGP is a funding source dedicated solely to securing transit assets has allowed the State of Connecticut to focus on this important issue. The TSGP has provided the much-needed funding to advance important security initiatives, such as the formation of a new Mass Transit Security Canine Unit within the Connecticut State Police. This unit is dedicated to transit and is part of DHS' operational initiative for visible, unpredictable, and deterrent efforts.

     The statewide "See Something, Say Something" public awareness campaign is another effective project that includes television, radio and newspaper spots to educate the public about being vigilant.

     Securing rail assets such as the New Haven Rail Yard through the installation of perimeter fencing, card activated gates, security guards, and other features also demonstrates an effective use of funding. This rail yard is the major maintenance yard for the New Haven Line rail equipment and is a critical asset. Other capital projects include the installation of security cameras at rail stations and on moveable bridges.

     Without the TSGP, and these projects funded by that program, there would be significant gaps in the overall security of rail lines, not just in Connecticut but in New York City as well. The New Haven Line terminates at Grand Central Terminal, which is a national landmark and icon. As security is strengthened in New York City, threats could be pushed out to feeder services where there may be a reduced security presence, therefore providing a means to attack targets in New York City.

- Some regional working groups are more competitive than cooperative, particularly when funding is on the line. How can TSA ensure that states and transit agencies stay focused on the security of the system as a whole?

  RESPONSE: It is important for TSA to ensure that smaller transit agencies such as Connecticut continue to receive a percentage of the funding under the TSGP. The challenge is to modify current federal grant criteria to include more proportionate funding for communities surrounding urban areas with connecting transit systems, rather than increasingly focusing transit grants almost exclusively within the city limits for large urban areas. The percentage of the funding needed for those surrounding communities with transit links is not large, but it must be sufficient for those communities to complete basic ongoing security measures already begun such as fencing, lighting, communications, and cameras.

- Your testimony suggests TSA and FEMA should consider using the Port Security Grant model when it comes to evaluating rail and transit grant proposals. What are the benefits of such a model?

  RESPONSE: Under the Port Security Grant model, the local Coast Guard Captain of the Port convenes a stakeholder group to evaluate and rank-order the grant applications. This provides critical local insight and prioritization to Headquarter administrators. The TSA Federal Security Director could serve an analogous function for the Transit Security Grant Program.

67123.128

Post Hearing Question and Response for the Record
Submitted to and Answered by the Honorable Peter J. Boynton
From Senator Mary L. Landrieu

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 22, 2011
Response submitted July 21, 2011

1. In your testimony, you stated that Connecticut had the 5th highest number of Visible Intermodal Protection and Response (VIPR) Team operations in the country in 2009, 34 in all, and that you expect the number of VIPR operations in your state to increase seven-fold by the end of this year. You also stated your belief that "support for VIPR transit security operations should be increased." As you may know, the President has proposed the creation of 12 new VIPR teams in Fiscal Year 2012, but the House decided not to include funding for these teams in their spending bill for the Department of Homeland Security. Please elaborate on the operational impact that VIPR teams have had in Connecticut, the types of capabilities they bring to the table, and their overall impact on security.

RESPONSE: My statement was making reference to the current level of VIPRs in 2011 being the fifth highest number in the country (not in 2009.) I was making the point that we have succeeded in increasing the number of VIPRs here in Connecticut, with TSA's help, from the modest number of 34 in 2009, to seven times that number this year, which, according to TSA, is the fifth highest number in the country this year. The overall impact of the VIPR operations is that they provide a random, uniformed presence for both real time security and deterrence. They add another layer of security but are not the only layer, and provide a presence for travelers and transit workers alike. The capabilities that VIPR operations bring to the table are the collaborative integration of TSA behavioral detection officers, uniformed police (local police departments); federal law enforcement (federal Air Marshals) and; State Police, including, in some cases, canine units.

67123.129

Post Hearing Question and Response for the Record
Submitted to and Answered by the Honorable Peter J. Boynton
From Senator Susan M. Collins

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 22, 2011
Response submitted July 21, 2011

1. How would you characterize the cooperation between federal, state, and local governments and the private sector in rail and surface transportation?

   RESPONSE: There is significant cooperation and interaction between federal, state, and local governments and the private sector towards developing a safe and secure environment within the transit system.

   MTA Police Department

   In Connecticut, the Metropolitan Transit Authority Police Department (MTA PD) is the primary law enforcement agency for Metro-North Railroad on the New Haven Line, responsible for policing thirty-six rail stations, patrolling the railroad right-of-way, and providing the primary response to all incidents in coordination with the Connecticut State Police and local police.

   Amtrak Police Department

   Amtrak Police is the primary law enforcement agency for the Shore Line East commuter service and Amtrak intercity passenger service in Connecticut. Amtrak has in place a program that includes a variety of security measures aimed at improving passenger rail security including uniformed police officers or Mobile Security Teams, random passenger and carry-on baggage screening, K-9 units, checked baggage screening, on-board security checks, and identification checks. Amtrak responds to incidents in this jurisdiction in coordination with the Connecticut State Police and local police.

   CT State Police, within the Department of Emergency Services and Public Protection

   Beginning in 2011, the Connecticut State Police's newly created Mass Transit Security Unit, consisting of a five-unit Canine Explosive Detection Team, conducts proactive explosive detection sweeps at passenger rail and bus stations/terminals and critical locations related to the mass transit system in Connecticut. The Unit coordinates with the Department of Transportation, MTA Police, Amtrak Police, various mass transit officials, federal agencies (including TSA VIPRs), and local police agencies involved in mass transit operations, and works to develop effective terrorism prevention strategies.

67123.130

Transportation Security Administration

The Transportation Security Administration (TSA) utilizes Visible Intermodal Prevention and Response (VIPR) teams to leverage resources quickly and to increase visible security in all modes of transportation. In Connecticut, VIPRs are utilized on the rails in collaboration with MTA PD and Amtrak PD. Typical Connecticut rail VIPRs include TSA, MTA PD, Amtrak PD, State Police including those Troopers deployed to the Division of Emergency Management and Homeland Security (DEMHS) within the Connecticut Department of Emergency Services and Public Protection, local police, and Connecticut National Guard personnel. VIPR teams are flexible in size and response. A VIPR at smaller platforms generally consists of 4-6 personnel, while VIPRs at larger stations typically consist of 10-15 personnel. In addition to visible deterrence, VIPRs in Connecticut also provide specially trained State Troopers assigned to DEMHS with advanced radiological and nuclear detection capabilities. TSA also provides a full-time on-site Intelligence Liaison Officer at Connecticut's Fusion Center, CTIC.

TSA also provides support for the Transit Security Grant Program and training.

FBI's Joint Terrorism Task Force

In Connecticut, the FBI Joint Terrorism Task Force (JTTF) includes members of various law enforcement agencies. These agencies provide intelligence information to the JTTF for investigation.

CT Department of Transportation

The Department of Transportation (ConnDOT) owns the two commuter rail services in Connecticut and ConnDOT contracts with MTA PD and Amtrak PD to provide police services on these lines. There is significant coordination with these agencies and local police in the towns where rail stations are located. There is ongoing planning and communication between ConnDOT and the newly created Mass Transit Security Unit within the State Police, which is a project funded through the TSGP. ConnDOT coordinates with TSA on VIPR initiatives and other security projects. ConnDOT is a member of the Regional Transit Security Working Group with New York and New Jersey transit agencies. This group collaborates on the TSGP and other security initiatives in the region. ConnDOT administers a number of transit security grants and works collaboratively with other stakeholders on transportation security issues, including serving as the co-chair of the Transportation Security Committee with all modes.

CT Division of Emergency Management and Homeland Security (DEMHS), within the Department of Emergency Services and Public Protection (DESPP)

DEMHS coordinates grants, planning and other homeland security-related activities with federal, state, local and private sector partners. The state's Fusion Center, the Connecticut Intelligence Center, operates within DEMHS, and is comprised of local, state and federal intelligence officers to receive, analyze, and disseminate intelligence information. The Critical Infrastructure Unit within CTIC assists in the coordination of VIPRs with TSA. DEMHS also coordinates and participates in the Transportation Security Committee established under the statutory authority of DEMHS and DESPP.

67123.131

US Coast Guard

The Coast Guard provides a part-time Intelligence Liaison Officer to CTIC, and also works to secure Connecticut's coastal waterways, including working with passenger/automobile ferries operating from Connecticut to Long Island (these two ferries are two of the fourteen largest ferries in the country, and are the only privately operated ferries among the fourteen, each carrying 1.3 million passengers per year.)

Other Stakeholders

State and local governments, passenger rail operators, and private industry are also important stakeholders in the state's rail security efforts. The state owns and operates a significant portion of the passenger rail system. The municipalities are directly affected by the rail systems that run within and through their jurisdictions. Consequently, the responsibility for responding to emergencies involving the passenger rail infrastructure often falls to state and local governments. State and local police participate in the VIPR initiatives in coordination with TSA, MTA PD, and Amtrak PD and respond to incidents along the rail line. Interoperable communications projects are also improving first responder communications among these agencies and the rail lines.

67123.132

Post-Hearing Questions for the Record
Submitted to Dr. Stephen E. Flynn
From Senator Mary L. Landrieu

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 22, 2011

1. **In your testimony you stated that "the public needs to know what they should be looking out for, who they are saying something to, and what they can expect as an outcome." You also mentioned Red Cross training, the Metro Citizen Corps established by the Washington, DC, Police Department, and Logan Watch as examples of programs that empower the traveling public and transportation system workforce to improve their ability to detect suspicious behavior and respond to it. What type of education, training, and skills should federal, state, and local authorities provide to better empower the public, and what are the best methods of delivery?**

The programs mentioned above perfectly highlight the ways in which the public can be engaged in a meaningful way. Metro Citizen Corps and Logan Watch provide a model for transportation authorities looking to leverage the potential of their industry partners and users. Providing everyday stakeholders with relevant tools and information can significantly enhance the efforts of professional operators who work to secure a system. Emphasizing civil society's ability to work alongside service providers should be a core mission of our homeland security effort.

The federal government should be much more forthcoming on sharing information about threat, vulnerability, and consequences to the rail and surface transportation sectors with the public, and more importantly, provide training on what to do when confronted with these threats and their consequences. The first preventers and first responders are more likely to be everyday citizens than the limited number of security and law enforcement professionals assigned to protect mass transit and surface transportation.

DHS should task its university-based Centers of Excellence to develop a training and education program in partnership with transportation companies and transit authorities. These companies and authorities, in turn, should be assigned the role as the primary delivery point for this training to transit and transportation users. Mandates with incentives for early adoption should be provided to transportation companies and transportation users to play this training delivery role.

67123.133

Post-Hearing Questions for the Record
Submitted to Dr. Stephen E. Flynn
From Senator Susan M. Collins

"See Something, Say Something, Do Something: Next Steps for Securing Rail and Transit"
June 22, 2011

1. **How would you characterize the cooperation between federal, state, and local governments and the private sector in rail and surface transportation?**

The federal agencies responsible for protecting this country, and their state and local counterparts, still need to do much more work to integrate, fully, the expertise of owners and operators of critical infrastructure and systems such as rail and surface transportation. Countering both natural and manmade threats most effectively and efficiently requires both a more open dialogue between federal officials and infrastructure experts and the implementation of truly cooperative, public-private, practitioner-guided programs that build infrastructure resilience.

In 2010, the Department of Homeland Security's Office of Infrastructure Protection announced a new project called the "Engagement Working Group" (EWG). The purpose of the EWG is to share classified information with representatives of the private sector in order to better develop strategies to counter threats to infrastructure. While this is a commendable effort, arguably there is a serious flaw with the program. Federal officials will provide security information only to vetted company security officers, who in turn are typically barred from relaying such information to executives and managers who do not hold active security clearances. As a result, investment and operational decisions are often made with little if any attention paid to the potential security stakes – especially for companies wherein security officers are not a part of the C-suite or where their recommendations are most often seen largely as cost with no return on investment. Furthermore, without well-tended relationships with decision makers beyond the corporate security office, federal officials will continue to miss out on critically needed insight and perspectives of industry leaders. DHS and the FBI should diligently work on finding the optimal "tear-line" that would allow more information that is currently classified or is designated at "Law Enforcement Sensitive" to be declassified and shared openly with industry leaders in the rail and surface transportation sectors.

67123.134

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
Homeland Security and Governmental Affairs Committee
Ten Years After 9/11: Preventing Terrorist Travel
Washington, DC
July 13, 2011

Good morning, the hearing will come to order. I want to welcome everyone to this, the fifth in a series of hearings this year that our committee is holding to review the state of our nation's terrorist defenses as we approach the 10th Remembrance of the attacks against America on 9-11-01.

Denying foreign terrorists the ability to travel to our country to attack us, as they did on 9-11, is obviously a continuing homeland security priority and is what we are focusing on today.

As you look back over the 10 years, and think of all that we've done to meet the challenge of preventing terrorists from coming into the country, we've done pretty well at it. There's not been another major attack from outside. And yet there have been attempted attacks in which people have shown they are still trying to enter the country, such as the cases of the shoe, Christmas Day and Times Square bombers. They all plotted outside the U.S. with help from al Qaeda and other Islamist terrorist groups and all involved travel into the U.S.

In the years since 9-11-01, legislation authored by this Committee has created a number of programs and systems meant to enhance our government's ability to identify and stop terrorists among the millions and millions of people who travel to the U.S. and who we want to welcome each year. The terrorists, obviously, we want to prevent from entering our country.

The "Homeland Security Act," which created the Department of Homeland Security, gave the new department the authority to set visa policy and deploy Visa Security Units to overseas consular posts and work with the State Department to provide an added layer of security in the issuing of visas.

The "Intelligence Reform and Terrorism Prevention Act of 2004," which was the original 9/11 Commission legislative implementation, called for a biometric entry and exit system for travelers into and out of the U.S., and also required enhanced travel documents. It required consular officials to conduct personal interviews with all visa applicants.

The 2004 Act also directed the President to negotiate agreements with other nations to share information on lost or stolen travel documents. And perhaps most important, it required that domestic and international airline passengers be screened against terrorist watch lists.

Then "The Implementing Recommendations of the 9/11 Commission Act of 2007," in a way the 9/11 Commission Act 2, created the Electronic System for Travel Authorization (ESTA), a program that allows the

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.135

Department of Homeland Security to screen travelers from so-called visa waiver countries against our intelligence and law enforcement databases before they board an airplane bound for the United States.

These programs are all critical new components of our post-9/11 effort to deny terrorists entry into the U.S. And I would say looking back, for the most part, they have been successful. But, as is documented in a series of reports from the Government Accountability Office (GAO), we clearly still have work to do.

First, some good news: GAO reports that the Electronic System for Travel Authorization has been well-implemented on our end and is helping to address gaps in the Visa Waiver Program.

In the same report, however, GAO says that only half of the visa waiver countries have signed the biometric law enforcement information-sharing agreements required for participation in the program, and none – not one – of these agreements has actually been implemented.

Looking back and forward, we need to get them all signed and all implemented – as quickly as possible.

The implementation of the US-VISIT entry system has really been one of the biggest success stories of our post-9/11 efforts. It ensures that almost all non-U.S. citizens coming to the U.S. have their fingerprints registered and are checked against all of our intelligence, immigration and law enforcement databases prior to being admitted. That's a very significant filter to stop terrorists from coming into the U.S.

Unfortunately, implementation of an exit system has been one of our biggest failures. GAO recently reported to this Committee that US-VISIT's current biographic system has a backlog of over 1.6 million records of potential overstays that have not been reviewed. In other words, these are people who have entered America legally, but overstayed the time during which they were legally authorized to be in this country. They become a very significant percentage of the millions of so-called illegal immigrants or undocumented aliens who are in our country. And this backlog is growing every day.

9/11 Commissioners Tom Keane and Lee Hamilton, in testimony before this Committee a few months ago, reiterated their call for a biometric exit system, and I look forward to hearing from our witnesses about the current plans at DHS for getting this done.

I also continue to be concerned with the slow implementation of the Visa Security Program. Although the Department of Homeland Security and the State Department have identified 57 high-risk consular posts abroad, only 14 of them have criminal investigators to provide an added layer of security to the visa issuing process.

The attempted Christmas Day bomber attack highlighted the importance of adequate security measures in place at our consular posts. But despite pledges by the Department of Homeland Security and the State Department to continue expanding this important security program, the President's budget included no additional funding for fiscal year 2012. Even in these admittedly tight budgetary times, that is disappointing.

GAO released another report yesterday that found a lack of coordination and focus in our government's efforts to help our foreign partners develop their own terrorist travel programs. That's something I'm sure we'll want to talk about today.

67123.136

Many of us on this Committee are concerned about security gaps in the Iraqi refugee program that allowed two Iraqi nationals, who turned out to be terrorists – one whose fingerprints turned up on an unexploded improvised explosive device that the FBI had in its possession since 2005 – to enter the country and then plot to send weapons back to their fellow terrorists in Iraq to use to attaek American troops there.

We need to know how these two were allowed to enter our country and why those fingerprints from 2005 were not entered into the system. Senator Paul has been particularly interested in this lapse, as these two Iraqi refugees found their way to his home state of Kentucky and I'm sure he'll have questions about it.

In sum, we have made significant progress in the past 10 years toward making the entry by terrorists into U.S. much more difficult than it was on 9-11-01. But we've had some very unsettling experiences that show they can penetrate the defenses we've set up. And of course we know the terrorists adapt their mode of operating to our increased security measures.

Just last week we saw reports that Al Qaeda is apparently even considering surgically implanting explosives inside the body of a person, which would be undetectable by most of our screening devices, but not by all of our defenses. Given these threats, we must continue to focus urgently on closing the gaps in our homeland security and that is what we will do today. I thank our witnesses for being here, as they are perfectly positioned to answer our questions today.

Opening Statement of
Senator Susan M. Collins

Ten Years After 9/11: Preventing Terrorist Travel

Committee on Homeland Security and Governmental Affairs
July 13, 2011

★ ★ ★

Limiting the travel of terrorists is a key way to protect our country. As the 9-11 Commission put it: "targeting travel is at least as powerful a weapon against terrorists as targeting their money."

According to the 9-11 Commission's report on Terrorist Travel, as many as 15 of the 19 hijackers might have been intercepted by border authorities if a procedure had been in place to share intelligence data.

At the time, however, threat information sharing systems and policies were largely absent, and the hijackers' past terrorist associations were not readily available to American officials who could have acted.

Today, we have a more rigorous system at high-risk consulates to help identify those who should not receive visas. But we need to upgrade the Visa Security Program so it can operate effectively and in more high-risk posts.

This program deploys additional Immigration and Customs Enforcement (ICE) agents to our high-risk embassies and consulates overseas to help identify suspected terrorists and criminals *before* visas are issued.

The problem is, the U.S. has these offices at only 19 posts, yet there are 57 high-risk posts. The GAO also has found ongoing turf battles between ICE and the State Department's Diplomatic Security at some posts.

VSP must implement effective procedures to help DHS and State Department agents resolve questions about who should—and who shouldn't—receive a visa to come to our country. All of those involved in the visa process at these high-risk embassies should be rowing in the same direction for the program to reach its potential.

There are other serious challenges and gaps in our security. Recently, we learned that terrorists intent on attacking America have shown interest in having explosive devices surgically implanted in their bodies.

67123.138

Yet, a young man was able to fly cross-country from New York to Los Angeles without a valid government ID and with an expired boarding pass that was not even in his name. And at the other extreme, it troubles many Americans to see the TSA putting the very young and the very elderly through intrusive, and in most cases unnecessary, pat-downs.

If we continue to give extra screening to individuals who pose no threat, yet others who should arouse suspicion can bypass check points without being questioned, our systems are still not properly calibrated.

As Senator Paul will discuss and as Republican Leader McConnell has highlighted, we also need to scrutinize the criteria for granting asylum.

In May, two Iraqi refugees living in Kentucky were indicted on federal terrorism charges. One of the men "allegedly carried out numerous improvised explosive device attacks against U.S. troops in Iraq," and the other also allegedly was an insurgent.

That they were permitted come to this country on humanitarian grounds is shocking.

How could this happen when there was sufficient evidence of the terrorist attacks to indict them?

What is being done to close this serious vulnerability?

Is the Administration re-analyzing the backgrounds of other refugees granted asylum under what appears to be a flawed process?

Even with improvements in our own safeguards, the U.S. cannot go it alone. Enhancing the capacity of other nations is a critical pillar supporting the strategy of combating terrorist travel.

A new GAO report, that I requested, provides an update on progress toward that goal. While the U.S. has many programs to help our partner nations improve their visa issuance and screening protocols, the GAO has found that too often these programs are not coordinated.

GAO also found redundancies. In one case, GAO discovered that in Pakistan, State and DHS were both planning to hold fraudulent travel document training for the same Pakistani agency during the same month without knowing of the other's plans.

These programs also do not focus sufficiently on corruption in the passport issuance process overseas, which, according to the GAO, is a significant obstacle in our efforts to keep terrorists from traveling.

There is some encouraging news. DHS reports that nearly 450 suspected terrorists have been identified on the watch list and blocked from boarding overseas flights bound for the U.S in fiscal years 2010 and 2011.

CBP is now matching passenger manifests with the terrorist watch list, and not just the "no fly" list. It is vital to review these lists before departure, not once the plane is airborne.

Terrorists constantly probe our defenses and innovate. We must never cease our efforts to keep terrorists from acquiring the documents and means to travel to our shores.

Statement for the Record

Rand Beers
Under Secretary
National Protection and Programs Directorate
And
Coordinator for Counterterrorism
Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
Washington, D.C.

Terrorist Travel

July 13, 2011

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members, I am pleased to appear before you to address what the Department of Homeland Security (DHS) has done to prevent terrorists from traveling to the United States. Our goal is to push information to the frontlines at the earliest possible point to prevent known or suspected terrorists from traveling to the United States. Today, I am testifying in two capacities. I am testifying as the Under Secretary for the National Protection and Programs Directorate (NPPD), a position I was appointed to by President Obama and confirmed by the Senate in June 2009. In this role, I have responsibility for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program and will speak to the tremendous work that organization is doing to validate identities and identify known or suspected terrorists. I am also testifying as the Coordinator for Counterterrorism at the Department, a role Secretary Napolitano assigned to me following the December 25, 2009, attempted bombing of Northwest Flight 253. I will address what the Department is doing to better coordinate its efforts to prevent terrorist travel, and describe the specifics of what US-VISIT activities are being done in this area. As this is my first testimony as the Counterterrorism Coordinator, I will also discuss why this role was created, how it has evolved, and the lessons the Department has learned since its creation.

Coordinating Terrorist Travel Screening

DHS collects and screens information on who is entering the country or boarding an aircraft in order to identify possible links to terrorist activity. U.S. Customs and Border Protection (CBP) has developed very sophisticated capabilities at the National Targeting Center as has the Transportation Security Administration (TSA) with Secure Flight. These advancements compliment the substantial progress that is being made across the federal government in accessing, sharing and vetting travel data. We continue to work closely with members of the

67123.141

Intelligence and Federal Law Enforcement Communities to further enhance our ability to prevent known and suspected terrorist from entering our country.

In this regard, the Department has made considerable progress since 9/11 to implement measures to identify and stop terrorist travel including:

- Unifying immigration and border management systems to implement a robust, effective, efficient, and timely capability to access and employ biometrie- and biographic-based information across the homeland security spectrum.

- Enhancing capabilities for more effectively identifying fraudulent documents and imposters and implementing measures to confirm document authenticity and validity.

- Establishing system interoperability and information sharing protocols with Federal partners and supporting State and local law enforcement agencies and the Intelligence Community. Working with our partners enables agencies to more effectively connect the dots and determine those who might pose a threat, through use of a more complete and accurate picture of a person's immigration, terrorist, and criminal history, as well as those that try to use more than one identity.

- Streamlining the visa overstay review process to establish reliable data on individuals who have violated the terms of their authorized admission.

- Establishing and maintaining strategic partnerships with an increasing number of international partners, sharing appropriate information, providing technical assistance, developing commonality in biometric standards and best practices, and investigating and testing emerging multimodal biometric technologies.

In the last few months, we have accelerated many of these efforts. In one notable example, the Secretary directed CBP, U.S. Immigration and Customs Enforcement (ICE), US-VISIT, U.S. Citizenship and Immigration Services (USCIS), Intelligence and Analysis (I&A), the Office of Policy, the Office of Operations Coordination and Planning (OPS), the Office of the General Counsel, the Privacy Office, and the Office of Civil Rights and Civil Liberties to come together to address the backlog of unvetted potential visa overstays identified by the Government Accountability Office in its April 2011 report. The goal of this ongoing effort is not only to identify which individuals have overstayed their visas, but also to prioritize investigation and removal actions for those that may pose a threat to national security. Since this effort began, DHS has used automated means to determine that of the 1.6 million potential visa overstays GAO reported in April, 843,000 are no longer in the country or have adjusted status. The remaining 757,000 are being vetted in three ways:

- First, US-VISIT, CBP and ICE are undertaking an initiative to run the overstay leads, both current and historical, through CBP's Advanced Targeting System (ATS). ATS has the ability to automatically check the records of potential overstays against other databases that can indicate a change in immigration status or a departure from the United States. Leveraging ATS yields an additional advantage of allowing the department to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00516 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.142

quickly gain greater insights on the background of overstay leads, which will assist ICE as it prioritizes leads with a potential nexus to a national security concern.

- Second, DHS will now provide overstay leads to NCTC to identify additional derogatory information held by the Intelligence Community.

- Third, DHS is now leveraging an existing data-sharing arrangement with the Intelligence Community to provide ICE with any additional matches of overstay leads with derogatory information.

This effort has helped to bring about a higher standard of review of overstay leads than previously existed, and at little cost. The process will allow ICE to better prioritize targets for investigation and removal. It is a prime example of how a coordination function can work in support of our operating components to better leverage information and capabilities spread across the Department and the interagency.

As part of the way ahead for DHS, we are focusing our efforts on improving information sharing, streamlining screening and vetting and identifying those who would do us harm while allowing the free movement of legitimate travelers. The Secretary, the Deputy Secretary and I look forward to working with you to make these improvements.

US-VISIT

Let me now address the work US-VISIT is doing to identify visitors to this country and to assist in the overall security of our immigration system. US-VISIT provides biometric identification and analysis services to distinguish people who pose a threat from the millions of people who travel for legitimate purposes. The program stores and analyzes biometric data—digital fingerprints and photographs—and links that data with biographic information to establish and then verify identities. US-VISIT's Automated Biometric Identification System, known as IDENT, is the Department's biometric storage and matching service, IDENT contains a watchlist of more than 6.2 million known or suspected terrorists, criminals, and immigration violators. This enables US-VISIT to provide homeland security decision makers with person-centric, actionable information when and where they need it, including at CBP primary screening where the fingerprints of all foreign nationals are run against the watchlist with results returned in under 10 seconds.

IDENT data, paired with biographic information from US-VISIT's Arrival and Departure Information System, support decision maker determinations as to whether foreign travelers should be prohibited from entering the United States; can receive, extend, change, or adjust immigration status; have overstayed or otherwise violated their authorized terms of admission; should be apprehended or detained for law enforcement action; or need special protection or attention, as in the case of refugees. IDENT plays a critical role in the biometric screening and identity verification of non-U.S. citizens for ICE, CBP, the State Department, USCIS, and the U.S. Coast Guard. US-VISIT is also working with other DHS components, such as TSA, to support their credentialing programs.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00517 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.143

US-VISIT's IDENT is fully interoperable with the Federal Bureau of Investigation's (FBI's) 10-fingerprint-based Integrated Automated Fingerprint Identification System (IAFIS). Daily transactions of FBI fingerprint data shared between IAFIS and IDENT number in the tens of thousands, providing the capability for FBI and US-VISIT customers to simultaneously match biometrics against our system, our watchlist, and FBI data.

Enhanced interoperability with the FBI has enabled US-VISIT to launch the Rapid Response capability, which allows CBP officers to search and receive a response against the FBI's entire criminal master file of over 69 million identities in near real time during primary inspection. Rapid Response is operational at four air ports of entry and is planned for nationwide deployment at air ports of entry next fiscal year.

DHS is also working closely with DOD to increase information sharing and establish interoperability between IDENT and DOD's Automated Biometric Identification System (ABIS). We currently have manual methods for sharing data. This helps DOD identify foreign combatants and match latent fingerprints retrieved from objects such as IED fragments or collected from locations where terrorists have operated.

The goal is to have the U.S. Government's three largest biometric systems—those of US-VISIT, the FBI, and DOD—completely interoperable, enriching our data sets, making information sharing more seamless and the biometric-checking process automated and far more efficient. While interoperable, the systems will continue to be maintained and guided by each agency's respective policies, including those to ensure appropriate privacy safeguards are in place.

International Cooperation and Collaboration

DHS works extensively with foreign governments to increase information sharing in order to prevent terrorist travel at the earliest point possible. The Department is focused on sharing appropriate information, increasing system interoperability, providing technical assistance, and establishing commonality in data and biometric standards and best practices. For instance, we are:

- Working with Mexican federal police and immigration authorities to identify and stop dangerous people from transiting Mexico, enhancing efforts to combat transnational crime and confront organizations whose illicit actions undermine public safety, erode the rule of law, and threaten national security, and supporting Merida Initiative capacity building programs such as the incorporation of biometrics into Mexico Immigration's Integrated System for Migration Operations.

- Forging new partnerships with New Zealand, India, South Africa, the Republic of Korea, Germany, Spain, Greece, and the Dominican Republic to support their implementation of biometrics.

- Sending technical experts to the United Kingdom, Australia, Canada, and, soon, New Zealand, to help build biometric capabilities and develop more systematic methods for information sharing.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00518 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.144

- Helping to implement Preventing and Combating Serious Crime agreements to formalize sharing of biometric and limited biographic data under the U.S. Visa Waiver Program with Germany, Spain and the Republic of Korea.

DHS will continue to expand international coalitions to protect our Nation in the face of evolving terrorist threats, an increasingly interconnected global economy, and growing transnational crime. Along with our partners, we view cooperation, collaboration, and information sharing as critical in reaching our common goals of enhancing global security while facilitating legitimate travel and ensuring access to our economies.

Success Stories

Interoperability and information sharing between agencies and international partners continues to yield significant results, as demonstrated by these success stories:

- On February 3, 2011, the Australian Department of Immigration and Citizenship submitted a batch of fingerprints under the High Value Data Sharing Protocol of the Five Country Conference for matching against IDENT. The fingerprints of a subject applying for asylum status in Australia matched an identity on the IDENT biometric watchlist as a known or suspected terrorist to the FBI's Terrorist Screening Database. US-VISIT contacted the FBI Counterterrorism Division and its Terrorist Explosives Device Analytical Center to confirm the subject's derogatory information. The FBI then notified Australian authorities. The individual was not granted his asylum status in Australia based on this information.

- In November 2010, US-VISIT assisted in a case regarding a Turkish man attempting to gain employment at a nuclear power plant. It was determined that the subject was using a false document under a false identity in an attempt to demonstrate his legal status to reside and work in the United States. The subject was subsequently arrested by local DHS law enforcement authorities as an overstay and placed into Federal custody awaiting removal proceedings.

- In October 2009, a vessel named *Ocean Lady* containing 76 undocumented males arrived off the coast of British Columbia, Canada. The intent of all individuals on board was to claim asylum status in Canada. The Canada Border Services Agency (CBSA) intercepted the vessel and worked with the ICE attaché in Ottawa to determine whether information on the identities of the individuals existed in U.S. systems. Pursuant to an existing agreement between CBSA and DHS, the asylum claimants' fingerprints were submitted to US-VISIT for a search. The fingerprint searches in IDENT identified matched to two subjects identified as known or suspected terrorists as members of the Liberation Tigers of Tamil Eelam. Both subjects had also previously applied for U.S. nonimmigrant visas in 2008 and had been denied.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00519 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.145

The Role of the Coordinator for Counterterrorism

Following the attempted attack on December 25, 2009, Secretary Napolitano assigned me an additional duty within the Department to improve coordination among the operational components and to bring together the policy and intelligence components to support this effort. As the Department's Coordinator for Counterterrorism, I am responsible for coordinating all counterterrorism activities for the Department and across its directorates, components, and offices related to detection, prevention, response to, and recovery from acts of terrorism.

In November 2010, DHS stood up the Counterterrorism Advisory Board (CTAB) to further improve coordination on counterterrorism among DHS components. As the Coordinator for Counterterrorism, I serve as the chair of the CTAB with the Under Secretary of Intelligence and Analysis and the Assistant Secretary for Policy supporting the Board as Vice Chairs. Members include the leadership of TSA, CBP, ICE, the Federal Emergency Management Agency, the U.S. Coast Guard, USCIS, the United States Secret Service, NPPD, and OPS. The DHS General Counsel serves as legal advisor to the CTAB and is present at all meetings.

As additional support for the CTAB, in December 2010, the Department also established a counterterrorism working group, known as the CTWG, to support the Coordinator for Counterterrorism and appointed a Principal Deputy Coordinator for Counterterrorism.

Our mission is aligned with the Department's central mission: to prevent terrorist attacks and enhance security. The Coordinator for Counterterrorism, the CTAB and the CTWG serve as the connective tissue that brings together the intelligence, operational and policy-making elements within headquarters and the components. We rely on I&A to provide an understanding of the threat and to coordinate with the intelligence components within the Department and within the Intelligence Community. We then facilitate a cohesive and coordinated operational response through the CTAB and other mechanisms so that we can deter and disrupt terrorist operations.

The CTAB is both headquarters-driven and component-driven. Components have the opportunity to engage in the Secretary's priorities in an organized, coordinated fashion, but also use the CTAB to bring attention to their initiatives and priorities that need support from other components and headquarters. The CTAB fosters collaboration among components and provides situational awareness of what each component does and needs from each other during a high-threat scenario. Similarly, we work with the Office of Policy to address long-term strategy issues that come out of this process and work to implement those changes. Let me provide two examples of how this process has worked over the last few months, with the offer to provide greater detail in a classified setting.

A few months ago, the Intelligence Community identified a potential threat to the Homeland. Over a series of interagency meetings, it was agreed that some mitigation measures needed to be put in place. Working within the Department, we put together a risk assessment to determine the most cost-effective way to mitigate the threat in the near term and then worked with our interagency partners to implement these measures. Now, the Office of Policy is working with our partners in the interagency to develop a long-term strategy to address the threat.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00520 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.146

Another example is how the Office of Policy engaged the Homeland Security Advisory Council to develop recommendations regarding the color-coded Homeland Security Advisory System. After the report was issued, Policy worked within the interagency to reach agreement regarding the development of a new system. In January 2011, the President directed the establishment of the National Terrorism Advisory System—or NTAS. Once the concept was finalized, the actual system was implemented and operationalized by the Coordinator for Counterterrorism, with the support of Operations Coordination and Planning within 90 days.

Soon after NTAS was up and running, we had the opportunity to test it following the death of Osama Bin Laden. While DHS did not issue an NTAS alert based on the threat of reprisal attacks or information obtained at Bin Laden's hideout, the CTAB met daily for the first week, sometimes multiple times per day. In each meeting, the CTAB considered whether any of the new threat information, when weighed against current preventative measures, met the threshold of being "imminent and actionable" to warrant the issuance of an NTAS alert. While none did, I&A worked closely with the FBI and our partners throughout the intelligence community to disseminate information as appropriate to the local law enforcement community and the private sector. Additionally, TSA engaged in extensive outreach efforts with airports, airlines, and freight carriers, and implemented a series of new security measures in the weeks following while CBP identified additional targeting measures to disrupt potential retaliatory attacks.

Conclusion

DHS has worked hard to stop terrorists before they ever get to the United States. As we continue to work to address today's complex challenges, we will look for innovative ways to bridge gaps between information, technology, and human decision-making. Working with our partners, using common technologies, standards, and best practices, and sharing critical information, will better protect us from those who seek to exploit our immigration systems.

By strengthening and increasing coordination within the Department, across the Federal government, and with our international partners, we will develop and implement comprehensive that make efficient use of limited resources. With the appropriate coordination and structure within DHS headquarters, we can better support our operational components as they work to enhance the security of our immigration systems while facilitating legitimate travel. In my role as Coordinator for Counterterrorism for the Department, I look forward to continuing to work with you to evolve this role and address the challenges that remain.

Chairman Lieberman, Ranking Member Collins, and distinguished Members, thank you again for this opportunity to testify. I will be happy to answer any of your questions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00521 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.147

DEPARTMENT OF STATE

WRITTEN STATEMENT

OF

JANICE L. JACOBS

ASSISTANT SECRETARY OF STATE FOR CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND

GOVERNMENTAL AFFAIRS

HEARING

ON

TEN YEARS AFTER 9/11: PREVENTING TERRORIST TRAVEL

JULY 13, 2011

Good afternoon, Chairman Lieberman, Senator Collins, and distinguished Members of the Committee. This is my third appearance before your committee on this important topic and I thank you for the opportunity to update you on the steps we have taken to increase the security of the visa process. I am also joined by my colleagues from the Bureau of Population, Refugees and Migration (PRM) and the Office of the Coordinator for Counterterrorism, who are here to answer your questions on these topics.

The Department of State (the "Department") is dedicated to the protection of our borders, and has no higher priority than the safety of our fellow citizens. We are the first line of defense in border security because the Department is often the first government agency to have contact with foreign nationals wishing to visit the United States. We are committed, with our partner agencies, to a layered approach to border security that will afford us the ability to track and review the visa eligibility and status of foreign visitors from the time they first apply for a visa and throughout their travel to, sojourn in, and departure from the United States.

Corrective Actions Implemented after December 25, 2009

After the December 25th, 2009 attempted terrorist attack on Northwest Flight 253, the President ordered corrective steps to address identified weaknesses in the systems and procedures we use to protect the people of the United States. In the months following the attack, we reviewed our "Visas Viper" requirements for reporting potential terrorists, as well as related visa issuance and revocation criteria, and introduced technological and procedural enhancements to facilitate and strengthen visa-related business processes.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00523 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.149

Our immediate focus was on the deficiencies identified following the attempted attack on Flight 253 by Umar Farouk Abdulmutallab. On the day following his father's November 2009 visit to the U.S. Embassy in Abuja, Nigeria, the Embassy sent a Visas Viper cable to the Department and the Washington intelligence and law enforcement community, stating that Abdulmutallab may be involved with Yemeni-based extremists. In sending the cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, and as a result of that misspelling, information about previous visas issued to him, and the fact that he held a valid U.S. visa, was not included in the cable.

At the same time, the Consular Section entered Abdulmutallab's name into the Consular Lookout and Support System (CLASS), our online database of lookout information. This correctly spelled CLASS lookout was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other agencies. On the basis of this CLASS entry, DHS's U.S. Customs and Border Protection (CBP) determined, after the flight departed Amsterdam, that Abdulmutallab warranted secondary screening upon arrival in Detroit. Additional reporting on this case carried the correct spelling, with additional reports reaching the same file in Washington.

After reviewing these events, we took immediate action to improve the procedures and content requirements for Visas Viper cable reporting. We directed all Chiefs of Mission to ensure that the Visas Viper program was working effectively at their posts, and that all appropriate agencies and offices at post contributed relevant information for Viper nominations. We instructed consular officers to include

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00524 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.150

complete information about all previous and current U.S. visas in Visas Viper cables. The guidance cable included specific instructions on methods to search comprehensively and intensively the database of visa records so that all pertinent information is obtained. We also issued new instructions to officers regarding procedures and criteria used in the field to revoke visas, and reiterated guidance on consular officers' use of the discretionary authority to deny visas under section 214(b) of the Immigration and Nationality Act (INA), with specific reference to cases that raise security and other concerns. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

In addition to changes in standard procedures for searching visa records, we immediately began working to refine the capability of our current systems, with a particular focus on matching records of currently valid visas against new and emerging derogatory information, to support visa revocation in appropriate cases. For visa applications, we employ strong, sophisticated name-searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in the 39 million records found in CLASS. This robust searching capability, which takes into account variations in spelling, has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We use our significant and evolving experience with searching mechanisms for derogatory information to improve the systems for checking our visa issuance records constantly.

CLASS has grown more than 400 percent since 2001 – largely the result of improved sharing of data among the Department, federal law enforcement agencies, and the intelligence community. Almost 70 percent of CLASS records

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00525 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.151

come from other agencies, including information from the FBI, DHS, DEA, and intelligence from other agencies. CLASS also includes derogatory information regarding known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the Terrorist Screening Center (TSC) and contains the data on KSTs nominated by all U.S. government sources. We automatically run all applicants' names against the Department's Consular Consolidated Database (CCD), which holds all our visa records, as part of our ongoing commitment to optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa holders. A system-specific version of the automated CLASS search algorithm runs the names of all visa applicants against the CCD to check for any prior visa applications, refusals, or issuances.

The Department has been continuously matching new threat information with our records of existing visas since 2002. We have long recognized this function as critical to the way we manage our records and processes. This system of continual vetting evolved as post-9/11 reforms were instituted, and is now performed by the TSC. All records added to the Terrorist Screening Database are checked against CCD to determine if there are matching visa records. Matches are sent electronically from the TSC to the Department of State to flag cases for possible visa revocation. In addition, we have widely disseminated our data to other agencies that may wish to learn whether a subject of interest has a U.S. visa.

Cases for revocation consideration are forwarded to us by our consular offices overseas, CBP's National Targeting Center (NTC), and other entities. As soon as information is established to support a revocation, a "VRVK" entry code showing the visa revocation is added to CLASS, as well as to biometric identity systems,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00526 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.152

and then shared in near-real time (about 15 minutes) with the DHS lookout systems used for border screening. As part of its enhanced "Pre-Departure" initiative, CBP uses these VRVK records, among other lookout codes, to recommend to airlines that certain passengers should not be boarded on flights bound for the United States. Almost every day, we receive requests to review and, if warranted, revoke visas for potential travelers for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours a day, seven days a week to address urgent requests, such as when a potentially dangerous person is about to board a plane. In those circumstances, the State Department can and does use its authority to revoke the visa prudentially, and thus prevent boarding.

The Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, the Department has revoked nearly 60,000 visas for a variety of reasons, including 4,000 for suspected links to terrorism; 1,320 of those occurring since the attempted attack on December 25, 2009 . Following that incident, we reviewed the last ten years of Visas Viper nominations, as well as "P3B" entries (potentially ineligible for a visa due to suspected ties to terrorism) in CLASS to determine whether Visas Viper subjects were properly watchlisted, and to determine the visa status of all P3B subjects. The Department's Visa Office completed a review of all 2001-2010 data and prudentially revoked thirty visas.

Because individuals' circumstances change over time, and people who once posed no threat to the United States can become threats, revocation is an important tool; we use our authority to revoke a visa immediately in circumstances where we believe there is an immediate threat. At the same time, we believe consultation

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00527 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.153

with national security partners is critical. Expeditious coordination with our national security partners is not to be underestimated. Unilateral and uncoordinated revocation could disrupt important investigations undertaken by one of our national security partners.

A More Secure Visa Application Process

The Department constantly refines and updates the technology that supports the adjudication and production of U.S. visas. Under the Biometric Visa Program, before a visa is issued, the visa applicant's fingerprints are screened against DHS's Automated Biometric Identification System (IDENT), which contains available fingerprints of terrorists, wanted persons, and immigration law violators, and against the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which contains more than 50 million criminal history records. In 2010, IAFIS returned more than 57,000 criminal arrest records to posts. The Biometric Visa Program partners with the DHS US-VISIT Program to enable CBP officers at ports of entry to match the fingerprints of persons entering the United States with the fingerprints that were taken during visa interviews at overseas posts and transmitted electronically to DHS IDENT; more than 10,000 hits are returned to posts every month from IDENT. (Not all IDENT hits result in visa refusals. For example, some records refer to deportations or voluntary removals that occurred up to twenty years ago, among other records that do not constitute any statutory ineligibility.) This biometric identity verification at ports of entry ensures the security of the U.S. visa by essentially eliminating the possibility of visa fraud through counterfeit or photo-substituted visas, or through the use of valid visas by impostors.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00528 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.154

We also use facial recognition technology to screen visa applicants against a watch list of photos of known and suspected terrorists obtained from the FBI's Terrorist Screening Center (TSC), as well as against the entire cache of visa applicant photos contained in our CCD. Facial recognition screening has proven to be another effective way to combat identity fraud.

The Consular Electronic Application Center (CEAC) is another major technological advance. CEAC is an electronic platform where applicants submit visa applications and photos via the Internet, eliminating paperwork, decreasing visa application and adjudication times, and reducing to one the number of forms applicants must complete. The worldwide rollout of the online DS-160 nonimmigrant visa application form is complete, and we are currently piloting the online DS-260 immigrant visa application form. These new online forms provide consular and fraud officers the opportunity to analyze data in advance of the interview, enhancing their ability to make decisions. They also afford intelligence and law enforcement agencies opportunities to analyze visa application data before applicants appear for their interviews. The online forms offer foreign language support, but applicants are required to answer in English, to facilitate information sharing between the Department and other government agencies. The new application forms are "smart," meaning that subsequent questions are triggered by an applicant's answers to earlier questions. The system will not accept applications if the security-related questions have not been fully answered, and "irregular" answers are flagged to ensure that officers address them in the interview.

In April 2011, we greatly enhanced the way we track visa fraud. We deployed globally a tool called the Enterprise Case Assessment Service that provides a

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00529 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.155

platform to store fraud-related research that used to be stored, for the most part, outside of consular systems. This new tool associates fraud-related information with visa records, making it available to consular officials around the world. Should fraud be confirmed during the course of a visa interview, consular officers can record that data in this new tool, where it can be easily referenced if the individual attempts to re-apply. Future iterations of this tool will track fraud in other consular services, such as U.S. passport applications, and will enable us to track the activities of third-party document vendors and visa fixers. We are exploring the possibility of sharing this new data source with our U.S. government partners to enhance interagency cooperation on fraud prevention.

Training

Consular officers are trained to take all necessary steps to protect the United States and its citizens during the course of making a decision on a visa application. Each consular officer is required to complete the Department's Basic Consular Course at the National Foreign Affairs Training Center prior to performing consular duties. The course places strong emphasis on border security, featuring in-depth interviewing and name-checking technique training, as well as fraud prevention. Throughout their careers, consular officers receive continuing education in all of these disciplines to ensure they integrate the latest regulations and technologies into their adjudicatory decisions.

Security Advisory Opinions

In addition, the Department's Security Advisory Opinion (SAO) mechanism provides officers with the necessary advice and background information to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00530 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.156

adjudicate cases of visa applicants with possible terrorism ineligibilities. Consular officers receive extensive training on the SAO process, including cultural and religious naming conventions, which assists them in identifying applicants requiring additional Washington vetting. The SAO process requires the consular officer to suspend visa processing pending interagency review of the case and additional guidance. Most SAOs are triggered by clear and objective circumstances, such as nationality, place of birth, residence, or visa name check results. In addition, in cases where reasonable grounds exist, regardless of name check results, to suspect that an applicant may be inadmissible under the security provisions of the INA, consular officers suspend processing and institute SAO procedures.

Consular officers refused approximately 23 percent of nonimmigrant and immigrant visas in FY 2010 (2,170,154 applications out of a total of 9,074,958 applications). The results of these checks by consular officers and any fraud indicators are brought to the attention of DHS's Visa Security Units and/or consular fraud officers wherever they are posted abroad.

The Visa Security Program

The Department of State believes that the Visa Security Program (VSP) is a valuable component of the U.S. government's overall policy of protecting our borders. We have a close and productive partnership with DHS, which has authority for visa policy under section 428 of the Homeland Security Act, and are fully supportive of the mission and future of the VSP, as well a number of data-sharing arrangements.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00531 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.157

The VSP maximizes the utility of the visa application and interview processes to detect and combat terrorism, criminality, and other threats to the United States and the traveling public. U.S. Immigration and Customs Enforcement (ICE) special agents assigned to Visa Security Units (VSUs) provide timely and valuable on-site vetting of visa applications and other law enforcement support to our consular officers. We work very closely with DHS to ensure that no terrorist receives a visa or is admitted into our country.

Reports from our VSU posts suggest that, as the VSP has matured over the past few years, VSU personnel have, where resources permit, moved beyond a singular focus on visa application review, and have been able to contribute their expertise and resources to enhance our response to all kinds of threats to the visa and immigration processes – terrorism, human smuggling and human trafficking, and trafficking in a wide variety of contraband. As reported by one of our missions, "(i)n addition to their concerns with visa security, [VSU agents'] efforts have also led to arrests and indictments in the areas of child pornography and countering the proliferation of controlled technology. This is a win-win partnership."

In Washington, we work very closely with our VSP colleagues on day-to-day issues affecting the operations of the program, as well as longer-term issues related to the expansion of the program to select overseas posts. VSP officers in Washington review our visa databases and advise posts of emerging information about visa holders. Another important aspect of our Washington partnership is the resolution of issues that are raised as the VSP expands to more posts. In January 2011, the Department's Bureaus of Consular Affairs (CA) and Diplomatic Security (DS) concluded a Memorandum of Understanding (MOU) with ICE. This MOU governs VSU-Department of State interactions within visa sections, procedures for

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00532 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.158

resolving the very few disputed visa cases that emerge from the VSU review process, and collaboration between ICE/VSU agents and their DS law enforcement colleagues assigned as Regional Security Officers (RSOs) or Assistant Regional Security Officer Investigators (ARSO-Is) assigned to consular sections.

Under the umbrella of section 428 of the Homeland Security Act and the corresponding Memorandum of Understanding between the Departments of State and Homeland Security, we work together to resolve cases. When warranted, DHS officers assigned to VSUs will conduct targeted, in-depth reviews of individual visa applications and applicants prior to issuance, and recommend refusal or revocation of applications to consular officers. We work with DHS to ensure that terrorists do not receive visas and to expeditiously revoke visas as appropriate.

The Department works collaboratively with DHS, pursuant to an October 2004 MOU between the Department and the ICE/VSP on the Administrative Aspects of Assigning Personnel Overseas, and National Security Decision Directive 38 (NSDD-38). This directive outlines factors to be considered when deciding whether establishing a VSU is appropriate at a particular post. NSDD-38 gives Chiefs of Mission responsibility for the size, composition, and mandate of U.S. government agency staff under his or her authority.

Currently, 19 VSUs are active at posts in 15 countries. Before submitting an NSDD-38 request, ICE officials, with the support of senior State Department officers from CA and DS, conduct a post-specific, on-site assessment. The visit provides an opportunity for the team to consult with officials at post to validate the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00533 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.159

interagency assessment of the risk environment, determine the feasibility and timing of establishing an office, and brief the COM on the role of the VSU.

Layered Security and Data Sharing

The Department embraces a layered approach to security screening. In addition to our support of the VSP, over the past seven years the Department and DHS have increased resources significantly, improved procedures, and upgraded systems devoted to supporting the visa function. DHS receives all of the information collected by the Department during the visa process. DHS's US-VISIT is often cited as a model in data sharing because the information we share on applicants, including fingerprint data, is checked at ports of entry to confirm the identity of travelers. DHS has broad access to our entire CCD, which contains over 143 million records, related to both immigrant and nonimmigrant visas, covering the last 13 years. A menu of reports tailored to the specific needs of each particular unit is supplied to elements within DHS such as ICE's agents assigned to VSUs.

We make all of our visa information available to other agencies, and we specifically designed our systems to facilitate comprehensive data sharing. We give other agencies immediate access to over 13 years of visa data, and they use this access extensively. For example, in May 2011, almost 22,000 officers from DHS, the Department of Defense (DoD), the FBI, DOJ, and the Department of Commerce submitted nearly two million queries on visa records.

Working in concert with DHS, we proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership with DHS and the FBI, we established the largest biometric screening

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00534 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.160

program on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. Currently, over 142 million images are enrolled in our facial recognition database. In 2009, we expanded use of facial recognition from a selected segment of visa applications to all visa applications, and we are now expanding our use of this technology beyond visa records. We are testing use of iris recognition technology in visa screening, making use of both identity and derogatory information collected by DoD. These efforts require intense ongoing cooperation from other agencies. We successfully forged and continue to foster partnerships that recognize the need to supply accurate and speedy screening in a 24/7 global environment. As we implement process and policy changes, we are always striving to add value in both border security and in operational results. Both dimensions are important in supporting the visa process.

In addition, we have 145 officers and 540 locally employed staff devoted specifically to fraud prevention and document security, including fraud prevention officers at overseas posts. We have a large Fraud Prevention Programs office in Washington, which works very closely with DS, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center in Williamsburg, Kentucky, and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging questionable applications and applicants who lack credibility, present fraudulent documents, or give us false information adds a valuable dimension to our visa process.

DS adds an important law enforcement element to the Department's visa procedures. There are currently 75 ARSO-I positions approved for 73 consular sections overseas specifically devoted to maintaining the integrity of the process.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00535 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.161

In 2010, DS approved 48 additional ARSO-I positions to work in consular sections overseas. They are complemented by officers working domestically on both visa and passport fraud criminal investigations and analysis. These highly trained law enforcement professionals add another dimension to our border security efforts.

The multi-agency team effort on border security, based upon broadly shared information, provides a solid foundation. At the same time we remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We have, and will continue to automate processes to reduce the possibility of human error. We are working and will continue to work to continually enhance our border security screening capabilities, and the contributions we make to the interagency effort.

We are facing an evolving threat. The people and the tools we use to address this threat must be sophisticated and agile and must take into account the cultural and political environment in which threats arise. The people must be well-trained, motivated, and knowledgeable. Information obtained from these tools must be comprehensive and accurate. Our criteria for taking action must be clear and coordinated. The team we use for this mission must be the best. The Department has spent years developing the tools and personnel needed to properly execute the visa function overseas, and remains fully committed to continuing to fulfill its essential role on the border security team.

Special Immigrant Visas for Iraqis

I am aware that the members of this Committee have a keen interest in Iraqi nationals working on behalf of the U.S. government in Iraq, who come to this

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00536 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.162

country as recipients of special immigrant visas (SIVs) or as refugees. More specifically, I know of your concern for the security of the process that brings them here. Following the recent arrest for terrorism activities of two Iraqis who arrived in the United States under the Iraqi refugee program, we are making special efforts to ensure the security of the SIV program as well as the refugee program.

The United States recognizes a special responsibility to Iraqis with U.S. affiliations and has developed several programs that can facilitate their access to resettlement in the United States. There are two categories of SIVs for Iraqis working for or on behalf of the U.S. government in Iraq. As of June 11, 2011, a total of 7,063 Iraqis have been issued special immigrant visas under the following two SIV programs – 1,629 Iraqis have been issued an SIV under the program established in section 1059 of the National Defense Authorization Act of 2006 for translators and interpreters, and 5,434 Iraqis have been issued a SIV under the program established in section 1244 of the National Defense Authorization Act of 2008 for other types of employment.

Many Iraqis who are eligible for a SIV opt to apply for the separate U.S. refugee resettlement program instead. As of June 22, 2011, over 59,000 Iraqi refugees have been resettled in the United States since 2007. We use 2007 as a starting point because Iraqis were not fleeing in large numbers until 2006, when the sectarian violence began in response to the bombing of the mosque in Samara. Under the law, an Iraqi applicant's spouse and minor children are also eligible for SIVs. Because some extended family members may be eligible under the refugee program, under exceptional circumstances, but not under the SIV program, the refugee resettlement program may be preferred by those who want their extended family to resettle together at the same time.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00537 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.163

We make every effort to streamline the SIV process where possible, while ensuring that Iraqi refugees and recipients of SIVs – like all of those who enter the United States – do not pose a threat to the security of the United States. However, implementing some of our newer security procedures has limited our progress in streamlining the SIV application process.

The Department is committed to issuing SIVs only to those qualified for the program. While we cannot discuss specifics for security reasons, SIV applicants from Iraq as well as Afghanistan undergo multiple layers of review. Over the past six months, we have worked with DHS and others to enhance the security screening process further to address potential security threats. In the past year, the Department of State, working with DoD and DHS, has continued to adjust our SIV application procedures to cut months off our processing times. We no longer require documentation that we found to be redundant; we have decreased the amount of paperwork that must be submitted by mail in favor of electronic submissions; and we have reorganized internal procedures so that the process moves faster. We are in the process of implementing additional improvements to be launched in the coming months.

Securing Refugee Admissions

In addition to its responsibility for the efficacy and security of the visa process, the Department is also responsible for the management of major parts of the U.S. Refugee Admissions Program, along with DHS and other U.S. federal and state agencies and offices.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00538 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.164

Every year, the United States admits tens of thousands of refugees as part of a humanitarian effort that reflects the highest values and aspirations of the American people, in a program that is authorized by Congress and historically has enjoyed broad bipartisan Congressional support. For decades, American communities have opened their hearts, homes, and neighborhoods to refugees from around the world. Our responsibility is to ensure that they do so with continued confidence in the security of the program.

Specifically, the Department's PRM Bureau, through its Resettlement Support Centers, conducts preliminary overseas pre-screening of refugee applicants for U.S. admissions, collecting pertinent biographic information necessary for numerous consular, law enforcement, and intelligence reviews. All refugee applicants for U.S. admissions are subject to the CLASS check and certain refugee applicants undergo the SAO check – both of which were discussed earlier in this testimony. DHS, which has final adjudicative authority for refugee admissions to the United States, coordinates numerous additional law enforcement and intelligence checks before granting admission to a refugee and his or her family.

The Department and DHS have taken a number of steps in recent years to strengthen the security screening of refugees, including through expanded intelligence community participation and elevated screening for certain refugee populations. We will continue to look for additional ways to enhance the security of this important humanitarian program.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00539 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.165

Training Foreign Passport Officials

As part of our fraud prevention efforts, Consular Affairs is working with the International Narcotics and Law Enforcement Affairs (INL) Bureau through INL's International Law Enforcement Academy (ILEA) network to provide passport antifraud training to officials from foreign passport issuance agencies.

The first class will be piloted in September 2011, in El Salvador for officials from various Central American countries. The training is designed to improve the integrity of other countries' passport issuance by helping them institute organizations, processes, and procedures for detecting fraudulent passport applications as part of their adjudication and issuance processes.

CA plans to offer this training at the ILEAs in Botswana and again in El Salvador in 2012.

Foreign Partner Capacity-Building Programs

The Department regularly engages our foreign partners bilaterally, regionally, and on a multilateral basis to address the issue of terrorist transit. This engagement involves a range of activities, including the exchange of information in a variety of security channels, the execution of capacity-building programs on border and document security, the provision of border screening programs like the Terrorist Interdiction Program/Personal Identification Secure Comparison and Evaluation System (TIP/PISCES), and through regular consultations on broader issues like we have with the EU and other capable partners. Our capacity-building efforts are intended to foster regional cooperation and collaboration, whether through

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00540 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.166

participation in organized regional groupings, such as the Trans-Sahara Counterterrorism Partnership, which facilitate regional training and exercises, or through assistance programs, such as the Regional Security Initiative, which funds regional CT training and cooperative efforts across all CT priority regions.

The Department works in close coordination with the interagency community for the development and implementation of the full range of counterterrorism programming, through a range of fora. In addition to participation in regular National Security Council-led meetings, we have established mechanisms, such as the aforementioned Regional Security Initiative (RSI), which brings together our Embassy leadership with the full range of interagency representatives to discuss key issues of regional concern. This is replicated at the working level through the Regional Interagency Consultative Group. In North Africa, as already noted, we also have the Trans-Sahara Counterterrorism Partnership, through which State, DoD, and USAID cooperate and coordinate efforts to strengthen the counterterrorism capacity of our regional partners. The success of this approach has led to consideration of a similar construct for other regions. In addition to coordination through formal structures, we cooperate informally on a regular basis with the Departments of Defense, Justice, Homeland Security and Treasury on our counterterrorism efforts across the board.

U.S. Government Efforts to Stop Terrorist Travel

The U.S. government has many programs designed to thwart terrorist travel around the world. Many portions of the U.S. government play a critical role in stopping terrorist travel – DHS and its components, DoD, law enforcement and intelligence communities, and State Department consular officers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00541 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.167

U.S. passports and visas contain sophisticated security features that make them very difficult to forge. State Department consular officers work with our partners from CBP and ICE to train foreign border and airline personnel in the detection of fraudulent travel documents. The Department's Office of the Coordinator for Counterterrorism (S/CT) also helps foreign partners at risk for terrorist activity to establish their own computerized stop-list systems via the TIP/PISCES program.

In the additionally critical areas of international travel document security and interoperability, we have intensified our work. With International Civil Aviation Organization (ICAO) member passport-issuing authorities around the globe, we have strived to ensure that, as with the U.S. passport, other issuing authorities meet internationally established standards for security and interoperability. This has included the cooperative and growing use of the Public Key Infrastructure (PKI), which is centrally managed and overseen by a board of ICAO member states that are active participants. Electronically reading the PKI, which assures the country name on the passport is the same country that issued the document, adds a third level of security for biometric passports, joining visual/tactile and laboratory features of the document, and scanner reading of the biometric content. This combination of features constitutes a tool bag for CBP officers to use in verifying the authenticity of the person and his/her passport when entering the United States.

The U.S. government's advance information-sharing initiatives ensure that we and our international partners are in constant contact regarding the threat of terrorist travel. CBP's use of Advance Passenger Information (API) and Passenger Name Record (PNR) data are valuable tools in detecting travel patterns and co-travelers of terrorist suspects. The U.S. government's agreements with foreign partners

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00542 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.168

under Homeland Security Presidential Directive (HSPD) 6 allow us to share terrorist screening information with trusted partners, in order to interdict known and suspected terrorists.

We also have entered into arrangements for the sharing of visa information with foreign governments, consistent with the requirements of section 222(f) of the INA. Since 2003, there have been arrangements in place with Canada for such sharing under certain circumstances. With DHS, the State Department is participating in a pilot program, through the Five Country Conference (United States, Australia, Canada, New Zealand, and the United Kingdom) for identification of travelers based on biometric matching in some individual cases. We are in negotiation with the governments of Canada and the United Kingdom for agreements that would provide a legal basis for us to implement arrangements for the automated sharing of visa refusal data and for systematic confirmation of an applicant's identity through biometric matching. These arrangements would be limited to information regarding nationals of third countries. We expect both agreements to be completed this year, and similar agreements with Australia and New Zealand next year.

The Department plays a key role in all of these international initiatives. With our partners at the TSC, we negotiate the HSPD-6 agreements overseas. We are a close partner with DHS in API and PNR discussions overseas, in particular with respect to the current talks with the European Union on PNR. Together, all of these programs are helping achieve the goal of constraining terrorist mobility. This is our obligation to the American people.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00543 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.169

Conclusion

We believe that U.S. interests in legitimate travel, trade promotion, and educational exchange are not in conflict with our border security agenda and, in fact, further that agenda in the long term. Our long-term interests are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Acquainting people with American culture and perspectives remains the surest way to reduce misperceptions about the United States. Fostering academic and professional exchange keeps our universities and research institutions at the forefront of scientific and technological change. We believe the United States must meet both goals to guarantee our long-term security.

Our global presence, foreign policy mission, and personnel structure give us singular advantages in executing the visa function throughout the world. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. national interests. The issuance and refusal of visas has a direct impact on our foreign relations. Visa policy quickly can become a significant bilateral problem that harms broader U.S. interests if handled without consideration for foreign policy equities. The conduct of U.S. visa policy has a direct and significant impact on the treatment of U.S. citizens abroad. The Department of State is in a position to anticipate and weigh all those factors.

The Department has developed and implemented an intensive visa application and screening process requiring personal interviews, employing analytic interview techniques, incorporating multiple biographic and biometric checks, all supported by a sophisticated global information technology network. We have visa offices present in virtually every country of the world, staffed by consular officers drawn

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00544 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.170

from the Department's professional, mobile, and multilingual cadre of Foreign Service Officers. These officials are dedicated to a career of worldwide service, and provide the cultural awareness, knowledge, and objectivity to ensure that the visa function remains the frontline of border security. Each officer's experience and individual skill set is enhanced by an overall understanding of the political, legal, economic, and cultural development of foreign countries in a way that gives the Department of State a special expertise over matters directly relevant to the full range of visa ineligibilities.

This concludes my testimony today. I will be pleased to take your questions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00545 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.171

WRITTEN TESTIMONY OF DAVID HEYMAN
ASSISTANT SECRETARY FOR POLICY
THE
U. S. DEPARTMENT OF HOMELAND SECURITY

before

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Ten Years After 9/11: Preventing Terrorist Travel

JULY 13, 2011
WASHINGTON, DC

Introduction

Chairman Lieberman, Senator Collins, and other distinguished Members, thank you for the opportunity to appear before the Committee to highlight the Department of Homeland Security's (DHS) work in preventing and countering terrorist travel. Preventing terrorists from traveling to or remaining undetected in the United States is a significant priority for the Department, and I commend the Committee for holding this and associated hearings, examining the progress that has been made since the tragic events of September 11th, 2001.

Ten years ago, screening of passengers coming to the United States was limited to the Department of State visa process, if applicable, and the inspection of a person by an immigration officer at the port of entry, plus whatever processes were applied at foreign airports and by foreign governments. Provision of advance passenger information was voluntary and, even when provided by air carriers, frequently contained inaccurate or inconsistent data. There was no biometric collection for visa applicants beyond photographs, nor for aliens seeking admission to the United States. There was very limited pre-departure screening of passengers seeking to fly to the United States and there was virtually no screening of any kind for domestic flights beyond airport checkpoints. There was no advance screening of passengers seeking admission under the Visa Waiver Program (VWP) and interagency sharing of information on terrorist threats was minimal.

Today, in response to both 9/11 and evolving threats, and with the help and support of Congress, we have significantly adapted and enhanced our ability to detect and interdict threats at the earliest opportunity. All air and sea passengers intending to travel to the United States under the VWP must now obtain an electronic travel authorization before boarding a carrier for travel to the United States through the Electronic System for Travel Authorization (ESTA) program, which screens passengers against various government databases and has virtually digitized the Form I-94W for authorized travelers from participating VWP countries. Additionally, all passengers seeking to fly to, from, or within the United States are similarly screened prior to boarding an aircraft under the Secure Flight program. For non-citizens, passengers' biometrics are collected and checked against terrorist watch lists prior to being issued a visa or being permitted to enter the United States, and agencies share information on known or suspected terrorists with each other. Further, we have developed new capabilities and systems (such as our Advanced Targeting System and Behavioral Detection program) to help identify possible terrorists who may be 'unknown' to us, but who seek to travel to or within the United States to do harm.

Since 9/11, however, the threat has changed to include not only large-scale attacks but also smaller operations with potentially catastrophic effects, such as continued targeting of the aviation sector. One example was attempted only a few weeks after I last testified before you on the subject of terrorist travel—the attempted bombing of Flight 253 on December 25, 2009.

Enhancements since December 25, 2009

Following that attempted bombing, the Department, in coordination with other components of the Administration, has worked to address issues and potential gaps that have been identified to ensure that we have a comprehensive and multilayered approach that begins abroad to detect and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00547 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.173

intercept terrorist travel and focuses on stopping terrorists at the earliest point before they can reach the United States. As represented by the other officials who have been asked to testify today on terrorist travel, we can see that this is truly an issue that requires significant collaboration and coordination among federal agencies.

It is important to point out that these improvements are not all directed at one area of the travel continuum—we must use a layered approach to strengthen security. As the 9/11 Commission pointed out, targeting terrorist travel is one of the most powerful weapons we have to counter terrorist operations. Terrorists travel in order to identify and engage in surveillance of potential targets; to plan their attacks; to train on tactics and operations; to collect funds and documents; and to communicate with other operatives. Every step along this pathway presents a vulnerability to would-be attackers, who must come out of the shadows and interact with the traveling public, the travel industry, and immigration and border security officials. At some point along the travel pathway, for example, many terrorists cross international borders—to communicate and engage others, train, or receive resources—a step that now necessitates submitting advance passenger information, using a passport and stopping at ports of entry.

Since 9/11, we have learned that preventing terrorist travel through immigration and border security is more than drawing a line in the sand where we can deny entry into our country. Rather, the exercise of immigration and border security authorities can be powerful resources used to identify and thwart terrorist operations at the earliest opportunity.

Accordingly, we have strengthened our security and screening at points:

- During the travel planning phase, when a traveler seeks a visa or authorization to travel;
- Just prior to travel, when a person seeks to board an aircraft at a point of departure; and
- During travel, when a person seeks to enter the United States.

I'll now discuss some of our recent improvements in screening across this travel continuum.

First, fulfilling a key 9/11 Commission recommendation, DHS fully implemented Secure Flight in November 2010. Under Secure Flight, DHS now prescreens 100 percent of passengers on flights flying to, from, or within the United States against the No Fly and Selectee portions of the U.S. known and suspected terrorist watchlist, and other specific data using passenger names, dates of birth, gender and, if applicable, redress numbers before travelers receive their boarding passes. In addition to facilitating secure travel for all passengers, this program helps prevent the misidentification of passengers who have names similar to individuals on government watchlists. Prior to Secure Flight, airlines were responsible for checking passengers against watchlists. Through Secure Flight, TSA now vets over 14 million passengers weekly. Approximately 25 individuals per month are denied boarding an aircraft through the Secure Flight program.

After the attempted attack on December 25, 2009, the United States also implemented threat-based screening measures to strengthen the safety and security of all passengers for air carriers with international flights to the United States. These new measures, which cover 100 percent of

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00548 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.174

commercial airline passengers traveling by air to the United States, utilize real-time, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

In addition, in 2010, DHS/TSA updated the Secure Flight program to use all terrorist watchlist records containing a full name and a full date of birth; travelers who are identified as a match against the terrorist watchlists are then designated for enhanced physical screening prior to boarding an aircraft.

DHS has also implemented the Visa Security Program (VSP) through which U.S. Immigration and Customs Enforcement (ICE) deploys trained special agents overseas to high-risk visa activity posts to identify potential terrorists and criminals before they obtain a visa to travel to the United States. The VSP is currently deployed to 19 posts in 15 countries. ICE special agents conduct targeted, in-depth reviews of individual visa applications and applicants prior to the issuance of a visa and recommend to consular officers refusal or revocation of applications, when warranted. Beginning in 2010, DHS began a new initiative with the Department of State where CBP recurrently vets *approved* visa applications so that as new information is discovered, DHS and the Department of State are able to proactively identify individuals who have visas and who may already be in the United States. To date, for fiscal year 2011, we have revoked 782 visas using this process, including 493 who were matches to the TSDB.

Additionally, DHS is continually working with interagency stakeholders to improve and expand procedures for vetting immigrant and nonimmigrant visa applicants, asylees, and refugees. The interagency vetting process in place today is more robust and considers a far broader range of information than it did in past years. Visa applicants, refugees, asylum applicants, and those seeking to enter the United States at a port of entry are subject to rigorous background vetting, biographic and biometric checks—including checks against records obtained from the Department of Defense in Iraq and Afghanistan. The security screening procedures for all of these categories have been enhanced over the past several years as vetting capabilities have evolved and interagency partnerships with the law enforcement and intelligence communities have been strengthened. Further, beginning last year, the Department began piloting a new recurrent vetting process for those applying directly to DHS for immigration benefits, similar to the process previously described for visas. As new derogatory information surfaces, we double-check those who have approved immigration status, such as refugee or asylee status, against this new information. These enhancements are a reflection of the commitment of DHS and other agencies to conduct the most thorough checks possible to prevent dangerous individuals from gaining access to the United States through the immigration process.

In addition, prior to the attempted terrorist attack on December 25, 2009, CBP conducted in-bound passenger targeting using Advance Passenger Information (API) and Passenger Name Record (PNR) data provided by the airlines, but could not easily prevent high-risk travelers from boarding flights to the United States unless they were traveling from a foreign location with an Immigration Advisory Program (IAP) or preclearance presence. After the December 25th attempted terrorist attack, CBP re-engineered its in-bound targeting operations to enable CBP to identify high-risk travelers who are likely to be inadmissible into the United States and to recommend to commercial carriers at <u>all</u> airports with direct flights to the United States that

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00549 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.175

those individuals not be permitted to board a commercial aircraft. Since the inception of this program—known as the Pre-Departure program—in January 2010, through mid-June 2011, CBP has identified 2,600 passengers who CBP determined would likely have been found inadmissible upon arrival to the United States.

DHS has worked closely with its intelligence and law enforcement counterparts to develop new mechanisms that identify high-risk applicants based on a broader set of data, including information that is not otherwise available to DHS or the Department of State. Similarly, since 2009, the U.S. Government has reformed the criteria and nomination processes for the terrorist watchlist and enhanced its information sharing capabilities so that measures now in place can comprehensively connect available pieces of intelligence to identify individuals who are known to be of security concern as well as people and connections that would otherwise remain unknown. Collectively, these enhancements help us to prevent dangerous individuals from entering the United States, and to support enforcement efforts within the United States if derogatory information develops after a subject of concern has already been admitted.

DHS has also strengthened the presence and capacity of law enforcement to prevent terrorist attacks on commercial aviation. Following the December 25 incident, DHS increased Federal Air Marshal Service (FAMS) coverage of U.S.-flag carriers' international flights through increased operational tempo by existing personnel. With the passage of the FY 2011 year-long continuing resolution, Congress appropriated sufficient funding to allow the FAMS to hire additional air marshals in order for the FAMS to return to pre-December 25 domestic coverage levels while maintaining existing heightened international coverage levels. The expanded FAMS program builds upon additional programs created since 9/11 that further increase the safety of aircraft, including the hardening of cockpit doors and allowing certain law enforcement officers to carry weapons on aircraft.

Building Bridges: International Partnerships, Information-sharing, and Interagency Cooperation

In addition to these recent enhancements and initiatives, there are several cross-cutting efforts that are worth pointing out that underlie all that we do to combat terrorist travel on a day-to-day basis. These efforts represent some of the critical linkages that that are vital for our daily operations to come together and work as a system, and not merely exist as the sum of the various parts. They include increasing international cooperation, sharing intelligence and participating in interagency information sharing, and using a multilayered approach to screening.

International Cooperation

To prevent terrorist travel we must work closely with our international partners—we must work bilaterally, regionally, and globally.

ICAO

In order to enhance global aviation security measures and standards following the attempted December 2009 attack, DHS initiated a broad international campaign to strengthen the global

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00550 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.176

aviation system against the evolving threats posed by terrorism. The first step of this campaign was to raise global awareness with key partners and allies.

Immediately following the thwarted attack, Secretary Napolitano and Deputy Secretary Lute contacted their Mexican, Canadian, and European counterparts to share information and solicit support for the need for aviation security enhancements worldwide. Subsequently, Deputy Secretary Lute and I traveled to meet with senior officials from 11 countries throughout the Middle East, Africa, Asia and Europe to lay the groundwork for improved aviation security standards.

In the weeks and months that followed, DHS worked with the International Civil Aviation Organization (ICAO) on an unprecedented initiative to strengthen global aviation against threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry. Secretary Napolitano participated in regional aviation security summits in Spain, Mexico, Japan, Nigeria, and in the United Arab Emirates, helping to bring about historic consensus with the international community to strengthen the civil aviation system through enhanced information analysis and sharing, cooperation on technological development, and modernized aviation security standards.

These efforts culminated at the ICAO Triennial Assembly in October 2010, where the Assembly adopted the Declaration on Aviation Security, which forges a new foundation for aviation security to better protect the entire global aviation system. The extraordinary global collaboration demonstrated by nearly 190 countries during the ICAO General Assembly has helped to bring about a truly 21st century international aviation security framework that will help make air travel safer and more secure than ever before.

This is not to say that there won't be new threats, or that there will be a new level of security overnight. To the contrary, this effort is foundational, but also transformational, and will lay the groundwork for a strengthening of the entire system over the next several months and years. It includes and underscores, for example, the critical value of analyzing travel data such as passenger name record or 'PNR' data and sharing information with our international partners in order to identify both known and unknown individuals traveling for purposes of terrorist training or committing acts of terrorism. It re-affirms the importance of working closely with our allies to identify those individuals who pose a risk but have not, until now, come to the attention of law enforcement or intelligence agencies. Every day, DHS prevents individuals seeking to travel to the United States by employing a number of tools that provide for advance information collection and analysis to identify potential threats. This process, which is a tenet of our own security, is now also one that has been embraced internationally as a result of our work over the past year.

VWP

The *Implementing Recommendations of the 9/11 Commission Act* of 2007 made even more explicit the connection between security cooperation and the VWP. Designation as a VWP member country provides tremendous incentives for countries to maintain high security standards and deepen their cooperation with the United States on security-related issues. The

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00551 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.177

cooperation that the VWP engenders - entry into agreements to share lost and stolen passport data with the United States through INTERPOL; sharing security and law enforcement information with the United States; cooperation on repatriation matters; the strengthening of document security standards; and airport and aviation security - helps secure the United States and prevent terrorist and criminal activities within VWP member nations, while also helping to facilitate and spur exchanges—commercial, tourist, and others—that benefit our economy, as well.

Due to these security requirements, all VWP countries now report lost and stolen passports to INTERPOL. This achievement, which contributes to the decreasing use of fraudulently-obtained passports, is a milestone and has contributed to the overall decline of fraudulent document intercepts at the border from VWP countries, from 712 in FY2004 to 36 in FY2010. In addition, 17 European countries have signed Preventing and Combating Serious Crime Agreements with the United States to share information about serious crime and terrorism, and negotiations with several other countries are in the final stages. These agreements enable each side to query the fingerprint databases of the other side for law enforcement purposes and otherwise enable each side voluntarily to provide data about criminals and terrorists. Also, VWP countries are required to enter into agreements under Homeland Security Presidential Directive (HSPD) 6 with the United States regarding the systematic exchange of identifying information on known or suspected terrorists and encounter management procedures. The Department of State and the Terrorist Screening Center have negotiated 15 of these agreements with European countries, and others are currently being negotiated.

PNR

As mentioned earlier, DHS analysis of Passenger Name Record (PNR) information – the information provided to the air carrier when booking international travel - is an indispensible part of transportation security and the prevention of terrorist travel. PNR data analysis assists in the identification of watchlisted individuals up to 72 hours prior to departure. DHS is then able to use PNR data to link previously unknown terrorists and criminals to known terrorists or criminals. Uniquely, our analysis of PNR allows us to identify high-risk travelers who have not previously come to our attention by matching them against travel patterns known to have been used by terrorists. The value of this technique is increasingly recognized internationally with other nations deploying or developing their own PNR systems. For some in the European Union (EU), however, this system has raised privacy concerns. As a result, DHS has concluded a series of four negotiations with the EU in the last decade to provide and maintain a legally certain operating environment to the airlines and to reassure our partners that DHS handles their citizens' data appropriately. Our most recent negotiation with the European Commission was concluded on May 16, 2011. The text, which represents an enormous amount of progress in terms of enhancing security and improving data protection, underscores the United States and the EU's continuing commitment to combat terrorism and serious transnational crime, while respecting both privacy and security. It must now be approved by the Council of the European Union and ratified by the European Parliament. While data continues to be utilized in the meantime, DHS encourages these bodies to quickly approve the agreement so its enhanced provisions may take effect.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00552 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.178

DHS has also worked with countries, including those in the Caribbean, to help them stand up passenger prescreening capabilities, focusing initially on Advance Passenger Information systems that will help them identify known illicit travelers.

North American Perimeter Security

DHS is also working to implement the President's February 2011 "Beyond the Border" declaration with Canadian Prime Minister Harper, which will strengthen North American security and make both Canada and the United States safer through a series of mutually beneficial initiatives. Specifically, we have jointly committed to taking a 'perimeter' approach to security in North America, and thus to collaborating to address threats well before they reach our shores. We will do so by developing a common understanding of the threat environment through improved intelligence and information sharing, as well as joint threat assessments to support informed risk management and targeting decisions. We will look for opportunities to integrate our efforts and where practicable, to work together to develop joint facilities and programs – within and beyond the United States and Canada – to increase efficiency and effectiveness for both security and trade. To increase travel security, counter fraud, and improve overall efficiency, we will also work together on an initiative to establish and verify the identities of travelers coming to North America and conduct screening at the earliest possible opportunity. This effort will include working toward common technical standards for the collection, transmission, and matching of biometrics that enable the sharing of information on travelers.

Capacity Building

In addition to screening travelers against derogatory information, it is important to ensure that officials also have the proper training and access to intelligence to detect fraudulent travel documents so that such documents cannot be used by terrorists seeking to subvert the screening process. The ICE Forensic Document Laboratory (FDL) is another tool in the arsenal against document fraud. The FDL is the federal government's only forensic crime laboratory dedicated exclusively to fraudulent document detection and deterrence. In partnership with the Department of State, the FDL provides training to international and domestic partners on identifying fraudulent documents.

DHS also works to implement significant programs around the world to provide training and technical assistance to build the capacity of foreign governments to confront terrorists, prevent terrorist movement, and strengthen our own security. DHS generally is not authorized to use its appropriated funds for foreign capacity-building purposes[1]; therefore, when our interests and priorities overlap, DHS works with the U.S. agencies that hold authority to fund foreign assistance, including capacity building efforts. These cooperative efforts to work with our international partners, and often to provide training and technical assistance, are based on where our assistance can help build a partner's capacity to combat terrorism. Some of these efforts

[1] There are a few exceptions for training the sharing of best practices by TSA in locations that have non-stop flights to the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00553 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.179

include: Border, Customs, and Immigration Police Training; Maritime Security and Seaport Interdiction; Civil Aviation Security and Reconstruction and Stabilization efforts.

Finally, DHS and the Department of State have worked with our closest allies to develop routine sharing of biometric information collected for immigration purposes. I will chair an initiative this year with the United Kingdom, Canada, Australia, and New Zealand that will build on these efforts and expand security and information sharing cooperation to mutually enhance travel security among our five countries. This type of cooperation, when implemented, can quickly reveal those who travel under multiple identities, or those who conceal their true identity in order to withhold pertinent information in an effort to obtain an immigration benefit. A new program that began in 2010, for example, which shares biometric information with the United Kingdom, Canada, Australia, and New Zealand, has identified many cases of routine immigration fraud, as well as dangerous people traveling under false identities.

As evidenced by this program, the information we gather and share with and from our international allies can be of great benefit. It also illustrates the importance of using all available resources to identify and prevent threats.

Intelligence and Information Sharing

The first critical step to thwarting terrorist operations along the travel pathway is to identify those associated with, suspected of being engaged in, or supporting terrorist or other illicit activities as well as the techniques they use to avoid detection. This is done by collecting, maintaining, and updating data and integrating knowledge of terrorist travel patterns into our immigration and border screening systems operations.

While watchlists existed prior to 9/11, they were neither coordinated nor consolidated to a degree and depth commensurate with what we now know to be the threat of terrorism. The 9/11 Commission recommendations and subsequent government hearings, reports and recommendations provided guidance to properly enhance this avenue for identifying and preventing the terrorist threat.

Four unique centers across the federal government provide critical resources to the Department's ability to understand, anticipate, and thwart terrorist travel. They have distinct areas of expertise and each serves a vital function for DHS. They are the Terrorist Screening Center, the National Counterterrorism Center, the National Targeting Center, and the Human Smuggling and Trafficking Center.

The Terrorist Screening Center (TSC), administered by the FBI, maintains the TSDB and provides information needed to help identify persons known to be, or reasonably suspected of being, associated with terrorism (referred to as "KSTs"). The terrorist watchlisting process incorporates biographic and biometric identifiers to support immigration and border screening. As an example, the TSDB maintains photographs of KSTs and makes this information available to the Department of State for screening visa applications. The broad range of terrorist watchlist information available and the ability to securely deliver it to the front line screening agency, overseas, at the border, or within the United States is a major improvement to the processes in place prior to 9/11.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00554 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.180

The National Counterterrorism Center (NCTC), by law, serves as the primary organization with the U.S. government for analyzing and integrating intelligence pertaining to terrorism and counterterrorism. Reporting to the Director for National Intelligence (DNI), it also serves as the central repository on KSTs and international terrorist groups. Pursuant to this authority, the Director of NCTC is responsible for providing strategic counterterrorism plans and effectively integrating and sharing counterterrorism intelligence inside and outside the United States. DHS has personnel assigned to the NCTC and utilizes the resources that the NCTC has at its disposal.

The National Targeting Center (NTC), run by CBP, provides tactical targeting information aimed at interdicting terrorists, criminal actors and implements of terror or prohibited items. Crucial to the operation of the NTC is CBP's Automated Targeting System, a platform used by CBP to match travelers and goods against screening information and known patterns of illicit activity often generated from successful case work and intelligence. Since its inception after 9/11, the NTC has evolved into two Centers: the National Targeting Center Passenger (NTC-P) and the National Targeting Center Cargo (NTC-C). The NTC analysts generate targets of interest or interdiction based upon the results of their research.

The Human Smuggling and Trafficking Center (HSTC) combats illicit and terrorist travel by bringing together experienced law enforcement, intelligence and diplomatic officials from U.S. agencies who are subject matter experts to work together on a full time basis to convert intelligence into effective law enforcement and other action. The HSTC combats illicit travel by:

- Facilitating the broad dissemination of all-source information;
- Preparing strategic assessments;
- Identifying issues for interagency coordination or action;
- Coordinating select initiatives; and
- Working with, and exchanging information with allied foreign governments and organizations.

ICE Homeland Security Investigations (HSI) plays a lead role in the U.S. government's attempt to identify, disrupt and dismantle foreign-based human smuggling organizations that pose a threat to U.S. security interests. It co-chairs a highly successful targeting project under the auspices of the Interagency Working Group on Alien Smuggling and Trafficking that identifies and prioritizes law enforcement action against the most dangerous smuggling organizations. In partnership with the Criminal Division of the U.S Department of Justice, HSI provides direct operational support under the Extraterritorial Criminal Travel Strike Force (ECT) program for the investigation and prosecution of these targets.

Layered Approach to Screening

As I mentioned earlier, DHS creates layers of defense by building security into each step of the transportation process and applying targeting techniques to the unique measures a terrorist traveler must take to get from one place to another.

An effective border screening system must include three reinforcing tracks: first, a consultative mechanism to ensure that an individual matched to a watchlist is in fact the person the U.S.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00555 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.181

government is interested in; second, a vehicle to accurately and reliably identify all travelers adopting known terrorist and criminal travel tactics even for which we do not yet have reliable identity information (e.g., name, passport number); and third, a way for innocent travelers incorrectly caught in the system to seek correction and redress.

DHS reviews the traveler's identity information and travel practices through six reinforcing systems:

a. The visa application process, for which DHS provides vital support to the Department of State.
b. ESTA, which determines eligibility of a person for travel under the Visa Waiver Program.
c. The Advance Passenger Information System (APIS), which allows CBP to compare the traveler manifest of commercial and private aircraft, as well as commercial vessels, against law enforcement databases, including the TSDB.
d. Secure Flight, which compares passenger information to the No Fly and Selectee List components of the TSDB.
e. PNR data, which analyzes information from the carriers' reservation systems to detect links to KSTs or patterns of criminal or terrorist activity.
f. The refugee application process through which DHS checks a myriad of systems in order to detect links to criminal or terrorist activity.

DHS obtains this information and begins conducting screening before an aircraft's departure. Combined, APIS and PNR data have assisted CBP in the identification of over 5,000 KSTs per year. These passengers were denied boarding, received enhanced security screening, or were removed from the watchlists after it was determined that they no longer posed a threat.

Additional Screening Mechanisms Used by the Department

A critical innovation of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No. 110-53) (9/11 Act) was the requirement for the development and implementation of an electronic system for travel authorization (ESTA) to determine in advance of travel the traveler's eligibility for VWP travel. ESTA was launched by DHS in August 2008 and, screens prospective VWP travelers against several databases, including the terrorist watchlist; lost and stolen passports (including INTERPOL's Stolen and Lost Travel Documents database); visa revocations; previous VWP refusals; and public health records. Since January 2009, nationals from all VWP countries, regardless of their port of embarkation, have been required to obtain an approved travel authorization via ESTA prior to boarding a carrier to travel by air or sea to the United States under the VWP.

DHS's U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program and the Automated Biometric Identification System (IDENT) database of biometric holdings support the Department's mission to protect our nation by providing biometric identification services to federal, state and local government to help them accurately identify the people they encounter and determine whether those people pose a risk to the United States. Upon arrival at a port of entry, alien travelers provide biometric data including fingerprints which are screened through

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00556 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.182

the DHS IDENT biometric watchlist, and also matched with previous biometric data collected from the person, such as during a visa application, to verify the person's identity.

DHS is committed to conducting rigorous screening in order to ensure that those being admitted to the United States, including those through the refugee program, are not seeking to harm the United States. Refugees legitimately are without documents that are needed to prove their identity. The Department has instituted rigorous screening methods to mitigate this vulnerability. In May 2007, DHS announced and implemented an Administration-coordinated, enhanced background and security check process for Iraqi refugees applying for resettlement in the United States. The security check regime, including both biographic and biometric checks, has been enhanced over the last several years as new opportunities and interagency partnerships with the law enforcement and intelligence communities have been identified. These enhancements are a reflection of the commitment of DHS and other agencies to conduct the most thorough checks possible to prevent dangerous individuals from gaining access to the United States through the refugee program. The latest enhancement to the refugee security check regime involves a new "pre-departure" check shortly before refugees are scheduled to travel to the United States. It is intended to identify whether any new derogatory information exists since the initial checks were conducted. These pre-departure checks went into effect in late 2010. No case is finally approved until results from all security checks have been received and analyzed.

As these enhancements which were initially designed for high risk refugee applicants have been implemented and proven valuable in identifying bad actors seeking to exploit our nation's immigration system, DHS has worked both internally and with our interagency partners—including the State Department and Intelligence Community—to expand these checks to certain other individuals seeking to travel or emigrate to the United States.

Enhancing background vetting for immigration benefits is an ongoing process. We are continuing to work with agencies that have potentially relevant data to determine whether and how to incorporate this information into the existing security check protocols for refugee applicants and others seeking immigration benefits or travel to the United States.

Conclusion

This nation has taken significant steps to counter and prevent terrorist travel since 9/11. They entail a multi-layered, many-faceted, and multinational effort that weaves together intelligence, information-sharing, security and law enforcement programs from across DHS, the interagency, and across a multitude of partnerships with our international and domestic partners. Together they reflect one of our nation's most pressing priorities: to ensure the safe and secure movement of literally millions of people traveling to, from, and around the United States on a daily basis, while thwarting the few would-be terrorists who seek us harm, at the earliest point in their journey.

Thank you again for this opportunity to testify. I look forward to answering any questions you may have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00557 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.183

Post-Hearing Questions for the Record
Submitted to the Honorable Rand Beers and and the Honorable David Heyman
From Senator Joseph I. Lieberman

"Ten Years After 9/11: Preventing Terrorist Travel"
July 13, 2011

Question#:	1
Topic:	terrorist travel
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: There are a number of programs at DHS that focus on preventing and interdicting terrorist travel, dispersed throughout the component agencies, the Office of Policy, and NPPD. These programs include, but are not limited to: Secure Flight, the Advance Passenger Information program, the Electronic System for Travel Authorization, the Visa Waiver Program, the Human Smuggling and Trafficking Center, the various trusted traveler programs, the refugee screening program, and US-VISIT.

Please provide a detailed explanation of how DHS coordinates the activities of these programs to ensure that they are working efficiently together to most effectively pre-screen travel to the United States and prevent terrorists from traveling.

Is any one entity or person at DHS in charge of ensuring that this coordination is taking place?

What are the mechanisms for ensuring that this kind of coordination happens?

Response: The Office of Policy coordinates and harmonizes the numerous and disparate credentialing and screening initiatives across the Department that are done to address the threat of terrorist travel. This role supports the legislative requirement that the Secretary "establish a program to oversee the implementation of the Secretary's responsibilities with respect to terrorist travel," under section 722 of *the Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53). Section 722 further outlines the designated officials in the Department of Homeland Security (DHS) Office of Policy for carrying out the program as well as the associated duties.

On a daily basis, DHS processes over one million inbound travelers at international ports of entry, as well as approximately two million domestic air travelers at 450 airports, conducts 135,000 biometric checks for visa applicants and individuals seeking to enter

67123.184

Question#:	1
Topic:	terrorist travel
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

the United States at border crossings, processes 30,000 immigration benefit applications, verifies the employment status of 60,000 new employees, manages a Trusted Traveler Program with over one million individuals enrolled, and processes 705 notices of arrival (vessels) in the maritime environment. All travelers are screened for terrorist ties, but not all screening is for terrorism. The Office of Policy works to promote a consistent and holistic focus on the entire spectrum of screening to make informed decisions about admitting a person into the United States, letting someone board a domestic flight, or issuing someone a secure card that carries with it privileges granted by the U.S. government.

Specifically, the Office of Policy's mission and responsibility is to strengthen homeland security by enhancing screening processes and technology to facilitate legitimate travel and trade; ensure individual privacy and civil rights and civil liberties are not diminished; ensure redress opportunities; and deter, detect, and deny access to, and/or withhold benefits from, those who pose a threat to the United States.

The Office of Policy accomplishes this as part of its broader screening coordination efforts to harmonize and enhance physical and information-based screening policies for all relevant DHS programs. The Office of Policy executes these responsibilities through three primary functions: the establishment of a screening framework, program advocacy, and portfolio management.

- *Screening Framework:* The Office of Policy develops screening policy for DHS and translates strategic guidance into implementation at the operational level for more than 40 screening programs of individuals. The office has issued several key strategic guidance documents to include the *Credentialing Initiative Report* and the subsequent *Credentialing Framework Initiative*, which analyzed the current credentialing environment and created a workable framework through which screening and credentialing programs can achieve strategic objectives and leverage the Department's best practices. The Office of Policy has also issued supporting policies such as the *Implementation of DHS Enterprise Standard for Core Person Biographic Data Elements, Enabling DHS Components to Create a Person-Centric View,* and the *DHS Policy for Physical Security Features*, which established consistent approaches to the collection of biographic data across programs and ensuring the development of secure documentation across the Department. The targets from the Credentialing Framework Initiative and the supporting policies are included in recently published DHS Integrated Planning Guidance documents that components use when developing their budgets. The Office of Policy also led DHS participation in the interagency revision of the Terrorist Watchlisting Guidance in response to gaps identified after the attempted attack on December 25, 2009.

67123.185

Question#:	1
Topic:	terrorist travel
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

- *Program Advocate:* In this role, the Office of Policy facilitates the development of screening policy decisions and project milestones for all relevant DHS programs; integrates programs into the DHS screening portfolio; and coordinates initiatives with all appropriate agencies and offices, both internal and external to DHS. Coordination may include both within DHS and the interagency, and routinely involves the DHS Offices of the General Counsel, Privacy, Civil Rights and Civil Liberties, Legislative Affairs, and other mission support offices. The Office of Policy ensures transparency and accountability, while allowing programs to proceed with their operational mission. It assists with White House and Congressional coordination concerning policies, programs, planning, operations, dissemination of information related to terrorist travel, as well as other people-screening related initiatives. The Office of Policy serves as the components' voice on screening at DHS Headquarters and communicates agency-wide decisions and approaches back to the components. For example, the Office of Policy worked closely with U.S. Customs and Border Protection (CBP) to ensure a successful implementation of one of their largest investments, the Western Hemisphere Travel Initiative.

- *Portfolio Manager:* As DHS's screening portfolio manager, the Office of Policy has a cross-cutting Department view of the more than 40 programs involved in various aspects of screening people. The Office of Policy serves as an integrator, making recommendations on budget and acquisition requests as screening programs move through the investment review process. The Office of Policy works closely with DHS's Office of the Chief Information Officer, the Acquisition Program Management Division, and Program Analysis and Evaluation office in the review of screening programs to ensure that the strategic direction, prescribed policies, and set targets are being supported through investment decisions. For example, the Office of Policy recommended that the U.S. Coast Guard (USCG) leverage TSA's established screening processes for screening individuals in the merchant mariner population, rather than USCG spending resources to develop its own vetting system. The Office of Policy works with other programs to leverage DHS enterprise services, establishing the Automated Biographic Identification System (IDENT) as the Department's biometric matching and storage capability and encouraging the expansion and fuller utilization of TECS, the automated system used by many Federal agencies for border enforcement needs and the sharing of border information.

As program advocate and portfolio manager, the Office of Policy ensures that opportunities to harmonize and automate enhanced screening processes across DHS

67123.186

Question#:	1
Topic:	terrorist travel
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

"people screening" programs re-use existing infrastructure, proven technologies, and resources already expended by the Department.

To advance these objectives, the Office of Policy regularly interacts with DHS components, including such as U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), the Transportation Security Administration (TSA), USCG, the National Protection and Program Directorate (NPPD)—including the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program and Infrastructure Protection, the Office of Intelligence and Analysis (I&A), the Visa Waiver Program, and with U.S. Citizenship and Immigration Services (USCIS) on a variety of transformational and operational programs. Similarly, the Office of Policy regularly interacts with interagency partners such as the Department of State (DOS), the Department of Justice (DOJ) to include the Federal Bureau of Investigation (FBI), the National Counterterrorism Center (NCTC), the Department of Defense (DOD), and the wider intelligence community to ensure that DHS programs and systems do not operate in a vacuum. Finally, the Office of Policy leads DHS representation to the National Security Staff Interagency Policy Committee (IPC) for Watchlisting and Screening, and participates in several other IPCs related to government-wide screening efforts.

67123.187

Question#:	2
Topic:	US-VISIT
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide the Committee with a detailed accounting for all of the money that has been spent to date by US-VISIT since the program's inception, including funding that was appropriated, obligated, expended, reprogrammed, and rescinded for:

Developing the Entry System;

Developing the Biographic Exit System, including specifying funding that was allocated for backlog reductions;

Developing a biometric exit system.

Response: Since its inception, the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program has been appropriated funding in each fiscal year (FY). At the end of FY 2011, US-VISIT plans to have a remaining balance of $27.4 million, which is "fenced" for the establishment of a comprehensive biometric exit program. The following table provides summaries for these appropriations, obligations, expenditures, reprogramming, rescinded funds, and remaining fund balance.

FY 2003 thru FY 2011 (Dollars in millions)	Appropriated	Obligated	Expended	Reprogrammed	Rescinded	Remaining Balance
Total	3,230.869	3,151.658	2,584.690	45.598	51.811	27.400

Note: The US-VISIT balance of $27.400 million is being rescinded in the 2012 Military Construction and Veterans Affairs and Related Agencies Appropriations Act in the General Provisions Section 572.

In FY 2007, US-VISIT received approval to reprogram $4.988 million from the development of the entry system to Identity Management and Screening Services (formerly referenced as Identity Services in the FY 2007 US-VISIT Expenditure Plan) to provide funding for a portion of un-reviewed overstay records.

In FY 2008, US-VISIT received approval to reprogram $40.6 million of prior-year appropriation funding. This approval allowed the reprogramming of $26.614 million from FY 2004 carryover funds and $13.968 million from FY 2005 carryover funds for additional funding to: 1) implement 10-print functionality; and 2) achieve initial operational capability for interoperability between the Department of Homeland Security Automated Biometric Identification System (IDENT) and with the Federal Bureau of

Question#:	2
Topic:	US-VISIT
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Investigation's Integrated Automated Fingerprint Identification System (IAFIS) by the end of FY 2008. The following table provides an accounting by appropriation, obligation, expenditure, reprogramming, rescissions, and balance of remaining funds for the entry and biometric exit systems as of July 18, 2011.

Dollars in millions	Appropriated	Obligated	Expended	Reprogrammed	Rescinded	Remaining Balance
Developing the entry system	705.800	688.014	428.487	17.786	-	-
Developing a biometric exit system	153.110	75.898	57.000	27.812	22.000	27.400
Total	**858.911**	**763.912**	**485.487**	**45.598**	**22.000**	**27.400**

The FY 2011 continuing resolution rescinded $32.795 million, $22 million of which was taken from the development of a biometric exit system.

FY 2003 - 2007 US-VISIT Expenditure Plans (Dollars in millions)	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010
Increment 1: Air and Sea	190.0	73.0	32.0	34.7	0.0	0.0	0.0	0.0
Increment 2A: Air, Sea, and Land	0.0	32.0	15.0	18.1	0.0	0.0	0.0	0.0
Increment 2B: Land	123.0	32.0	0.0	0.0	0.0	0.0	0.0	0.0
Increment 2C: Border Technology and Infrastructure	0.0	49.0	55.0	0.0	0.0	0.0	0.0	0.0
Increment 3: Land	0.0	53.1	25.0	0.0	0.0	0.0	0.0	0.0
Entry/Exit	0.0	0.0	0.0	0.0	7.3	0.0	0.0	0.0
U.S. Travel Documents and e-Passports	0.0	0.0	0.0	16.1	10.8	0.0	0.0	0.0
Comprehensive Exit	0.0	0.0	0.0	0.0	0.0	13.0	0.0	22.0
Total	**313.0**	**239.1**	**127.0**	**70.9**	**18.1**	**13.0**	**0.0**	**22.0**

US-VISIT has been appropriated approximately $858.91 million for entry and exit. Enhancements to the Arrival and Departure Information System support both entry and exit purposes.

Question#:	3
Topic:	exit system
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Committee continues to be concerned about the Department's commitment to deploying a comprehensive exit system to identify individuals as they leave the country. NPPD has a statutory mandate to develop a viable exit system. Undersecretary Beers testified before the Committee in December of 2009 that US-VISIT was close to a decision on how to proceed with the exit portion of the system. During the first hearing in this series, 9/11 Commissioners Keane and Hamilton reiterated their call for biometric exit system as being fundamentally important. Nearly a decade after 9/11 we lack a comprehensive exit system of any kind—biometric or biographic, as GAO has recently reported that the current biographic exit system continues to be riddled with problems and is not effective.

Please provide the Committee with a detailed timeline for implementing the exit portion of US-VISIT to all ports of entry.

Please address the GAO findings that paper I-94 forms continue to be issued but that they are not used to calculate overstays in the air environment and are not systematically collected at the land border. Are these forms still needed? How much money does DHS spend on the I-94 program?

When will DHS formally announce its decision concerning its goal for implementing the biometric exit system required by law?

Has DHS explored using alternate biometrics, such as facial recognition, to verify exit?

Please explain for the Committee how DHS plans to improve the biographic exit system in order to ensure that overstay data is reliable and to address the GAO's concerns.

Response: Deploying a biometric exit system in the aviation environment alone has been estimated to cost between $3 and $9 billion, depending on the collection mechanism. Developing biometric exit systems for land borders would also require substantial investments. DHS is currently researching methods, through our Science and Technology Directorate, to deploy biometric exit and is focused on ways to improve the efficiency and cost effectiveness of collecting the biometrics. Facial recognition is certainly one of the biometric tools DHS continues to explore. However, the current budgetary environment makes a significant investment in biometric exit not feasible for the Department at this time.

67123.190

Question#:	3
Topic:	exit system
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

In the meantime, however, DHS is enhancing its existing biographic exit program, which provides similar benefits as biometric exit, but at a greatly reduced cost. Through the biographic exit program, passenger information is transmitted by air carriers to DHS via CBP's Advance Passenger Information System (APIS) program and then recorded into the US-VISIT Program's Arrival and Departure Information System (ADIS) system. APIS requires commercial air and commercial sea carriers to provide manifest information for all travelers departing the United States on board their conveyance. APIS data for visitors is provided to US-VISIT ADIS for departure matching.

Currently, the DHS biographic exit program provides evidence for sanctions against those who overstay and thus violate immigration law: persons are deemed inadmissible and placed on overstay watchlists, visas are cancelled, and other actions are taken. The proposed enhancements to our existing biographic exit program are as follows:

a) Reviewing and eliminating the existing unvetted overstay records: As of May 2011, there were 1.6 million biographic records where a departure was not matched to an arrival record indicating a possible overstay, as the GAO report noted. Through a new automated review process, comparing these records to ADIS and the USCIS Computer Linked Application Information Management System (CLAIMS), 863,000 records are no longer considered potential overstays through information discovered from those systems. The remaining 757,000 records require a manual review to determine if the record is truly an overstay, or if the traveler actually has, in fact, departed or lawfully extended his or her status. A full review of outstanding overstay records will ensure all records are checked against the Department's targeting rules and also establish a country-by-country overstay rate with high fidelity.

b) Matching all overstay records against CBP's targeting rules: As discussed above, the automated and manual reviews against CBP's targeting rules are ongoing, and from a security standpoint, will enable DHS to take action against those who have overstayed within priority enforcement areas. All overstay records are vetted against the holdings of the National Counterterrorism Center (NCTC) and others in the Intelligence Community.

c) Technical Enhancements to CBP's APIS and NPPD's ADIS systems: The APIS system enhancements will allow DHS to more readily determine if there are deficiencies in data provided by the airlines. APIS will utilize interactive communications to alert air carriers when the APIS information provided is unable to be validated against source information held by DHS such as a Lawful Permanent Resident card, non-immigrant visa, ESTA or U.S.-issued passport. Validation will occur for both arrival and departure manifest submissions, allowing for better

67123.191

Question#:	3
Topic:	exit system
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

matching of biographic records while maximizing the chances of automated matches, negating the need for more costly manual reviews in the future. ADIS enhancements will include better and faster access to immigration benefit data held by USCIS, which will increase the accuracy of identifying overstays in an automated way, reducing the cost and time of reviewing cases manually.

DHS will deploy a biometric exit program and, when doing so, will ensure it is a responsible use of taxpayer funds. Under the current financial climate, now is not the appropriate time. Nevertheless, DHS is pursuing a research program to identify ways in which biometric exit could be deployed, at lower cost, through technology enhancements that fit within the operational environment DHS requires. In the meantime, DHS will continue to enhance its existing biographic exit program, which will allow DHS to better identify overstays than it can now and sanction them.

Regarding I-94 forms, these documents are used to document lawful presence and the terms of admission, including the time of admission granted to an individual presenting a visa to enter the United States. They are used for other reasons than to calculate overstays of foreign nationals. DHS is currently evaluating options for transitioning to a paperless I-94.

Question#:	4
Topic:	GAO
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: A GAO report requested by this Committee revealed that DHS had a backlog of 1.6 million potential overstays that had been identified by an automated system but that had not been further examined to ascertain whether the individuals in question had actually left the country or adjusted status. During a May hearing, Secretary Napolitano testified that DHS had requested additional funding in FY2012 to deal with the backlog. Two months later, Undersecretary Beers testified that the backlog would be cleared by early August.

Please provide the Committee with a detailed explanation of how DHS currently identifies potential overstays.

Response: The National Protection and Programs Directorate's U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program uses the Arrival and Departure Information System (ADIS) to match biographic data on arrivals, departures, extensions, and changes or adjustments of status to identify individuals who may have overstayed the terms of their admission. The system uses visitors' "admit-until dates" to indicate whether they may have remained beyond their authorized periods of admission. Overstay records that ADIS identifies as in-country are prioritized and reviewed using U.S. Immigration and Customs Enforcement (ICE) guidelines for overstay records-of-interest based on national security and intelligence criteria. All other records are considered to be non-priority.

In-country overstays are individuals who may have exceeded their periods of admission and remained in the United States. Minor records, a subset of the in-country overstay records, are for individuals who have overstayed, but who are under the age of 18, which is the minimum age for ICE Counterterrorism and Criminal Exploitation Unit (CTCEU) processing of overstay records. Minor records are not processed manually but are batched and forwarded to CTCEU weekly. Currently, priority in-country overstays undergo three additional automated processes in sequential order:

- *Additional ADIS searches:* This automated process allow for multiple searches of ADIS to highlight any changes in information or multiple person identifications.

- *Computer-Linked Application Management Information System (CLAIMS) search:* This process searches CLAIMS for any records that match recent immigration benefits applications, such as an extension of stay or adjustment of

67123.193

Question#:	4
Topic:	GAO
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

status, that were not sent to ADIS and that may have impacted a traveler's admit-until date and/or immigration status.

- *Automated Targeting System (ATS) search:* This process searches ATS for I–94 records that ADIS may not have located.

Historically, these automated processes reduce the number of overstay records by 40 to 45 percent. Overstay records that cannot be closed during automated processes are then manually validated by US-VISIT analysts to ensure that only credible leads are forwarded to ICE. During the manual validation, US-VISIT analysts review information from an additional 12 Government systems. Records that cannot be closed after manual review are transmitted to ICE as in-country overstay leads.

The Department of Homeland Security (DHS) will use an enhanced process, leveraging an arrangement with the National Counterterrorism Center, to vet future overstays from a public safety and national security perspective. In addition, DHS is reviewing a range of options to automate the system searches conducted during the manual vetting of overstays to enhance overstay review from an immigration status and location perspective. It is anticipated that this could reduce the number of manual system queries that need to be performed. Once the review is complete, DHS will be able to identify the potential efficiencies and resource implications through the automation of system searches.

Out-of-country overstays are individuals who stayed beyond their authorized periods of admission, but who have departed the United States. For out-of-country overstay records, if the overstay event is confirmed, both biographic and biometric lookouts are created for these individuals respectively in the CBP TECS database and in US-VISIT's biometric database, the Automated Biometric Identification System (IDENT). The lookouts are then available to CBP officers, if an overstaying individual attempts later to re-enter the United States at a port of entry, as well as to Department of State consular officers if the individual were to reapply for a visa to the United States at a consular office overseas.

Question: Why did DHS allow a backlog in processing potential overstays to develop, if it could be cleared so quickly?

Response: The unreviewed overstay records dated back to 2005. US-VISIT used ICE guidelines based on national security and intelligence criteria to prioritize its review of overstay records. The non-priority records accumulated in a queue are pending future

67123.194

Question#:	4
Topic:	GAO
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

processing. However, the records were filtered, over time, through an established automated query to reduce the number of system identified overstay records.

Recognizing that the vulnerability identified by Congress required a Department-wide approach, DHS drew on the recently maturing, cross-Component coordinating ability of the DHS Counterterrorism Coordinator to bring together parties to identify a solution.

Question: Please provide the Committee with a detailed explanation of how the backlog was cleared so quickly.

Response: In May 2011, at the direction of Secretary Napolitano, DHS's Office of the Counterterrorism (CT) Coordinator organized an effort to ensure that all overstays, regardless of priority, receive enhanced national security and public safety vetting by National Counterterrorism Center (NCTC) and U.S. Customs and Border Protection (CBP).

US-VISIT performed an automated validation of the 1.62 million records in the backlog, reducing it to 757,000 possible in-country overstays. Both NCTC and CBP vetted the remaining 757,000 potential, in-country overstay leads, along with 82,000 previously vetted overstay leads, for national security and public safety concerns. CBP utilized its Automated Targeting System to query multiple databases and to compare records to CBP's intelligence-based threshold targeting rules to identify such indicators as suspicious travel patterns or anomalous travel behavior. Simultaneously, NCTC vetted the backlogged records through a number of databases.

By the end of July 2011, all possible overstays in the previously un-reviewed records had been reviewed from national security and public safety standpoints. ICE has begun investigation of these records of concern.

Question: How does US-VISIT plan on ensuring that another backlog does not develop?

Response: The DHS FY 2012 budget request includes additional resources that will allow US-VISIT to review all potential overstay records. DHS will use the enhanced process, identified above, to vet future overstays from a public safety and national security perspective. In addition, DHS is reviewing a range of options to automate the system searches conducted during the manual vetting of overstays to enhance overstay review from an immigration status and location perspective.

Question: When US-VISIT first began examining its backlog of potential overstays, did it discover any individuals on the backlog who were associated with terrorism or serious

67123.195

Question#:	4
Topic:	GAO
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

crimes? If so, please provide the Committee with the specific details of each of these cases, including how they were ultimately resolved.

Response: The 757,000 overstay records were vetted against intelligence-based targeting rules developed by U.S. Customs and Border Protection, in addition to criminal history, the Terrorist Screening Database, and other hits identified in the Automated Targeting System, resulting in almost 3,000 potential matches. Over 800 leads have been identified and 50 of those leads have been referred to the field for investigation. The criminal history results are still being analyzed for public safety and national security concerns.

In addition, the vetting of the 757,000 records revealed derogatory information by the National Counterterrorism Center on 15 unique individuals. The current status provided by ICE of those individuals are as follows:

- Six were determined to be non-immigrants who are outside of the United States.
- Three had applied for asylum. Two of these applications are pending and one was ruled ineligible and is in removal proceedings.
- One is a lawful permanent resident who is currently outside of the United States.
- Four are active in the Student and Exchange Visitor Information System, including two subjects whose visas have been revoked.
- One individual appears to be present in the United States and is currently the subject of an ongoing investigation.

67123.196

Question#:	5
Topic:	overstay rate 1
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The President recently endorsed a bill that would use the overstay rate instead of the visa refusal rate as the benchmark for allowing new countries to join the Visa Waiver Program.

What improvements need to be made to US-VISIT before it can provide us with an accurate overstay rate that Congress could have confidence in?

Response: For DHS to provide accurate overstay rates, the following improvements are required:

a) CBP/ATS-P Automated Interface

1. Automates current manual intensive process between CBP/US-VISIT/ICE
2. Provides enriched overstay data directly into ADIS Overstay Management Tool (DIIV)
3. Provides data integrity improvements to ADIS by providing additional updates from ATS-P system sources

b) ADIS/IDENT Interface Upgrade

1. Provides travel history and change of the status updates to ADIS by importing IDENT data
2. Reduces the overstay list by improving data integrity of ADIS
3. Closes information gaps at US-VISIT between ADIS and IDENT

c) USCIS Transformation IOE Interface

1. Provides ADIS with needed interface to receive changes in immigration status updates beyond current connectivity to USCIS (CLAIMS3)

d) Lawrence Livermore National Labs (LLNL) Matching Enhancement

1. Incorporates biometric identifier(s) into biographic matching for enhanced entity resolution in ADIS (Confidence in ADIS vs. IDENT Identities Gap)

Question: How long does a person need to overstay their admission period for in order to count as an official overstay (e.g. 1 day over legal admission period, 30 days, 90 days, etc…)?

67123.197

Question#:	5
Topic:	overstay rate 1
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Response: Pursuant to existing statutes, any overstay results in the automatic cancellation of the person's visa, ESTA approvals (if any), and the inability of the person to use the Visa Waiver program (VWP) ever again. If the overstay period is beyond 180 days but less than 1 year, the person is statutorily inadmissible for a period of three years; if the overstay period is more than one year, the inadmissibility period is ten years. In these cases, the person could not lawfully be admitted to the United States without a waiver. In addition, at any time beyond a person's lawful period of authorized stay, that person is subject to removal from the United States and not lawfully permitted to work. An individual is officially listed as an overstay when he or she has stayed one day beyond his or her period of admission.

Question: Has DHS attempted to introduce statistical significance into its calculations of overstay rates? What would this entail?

Response: Tests for statistical significance are generally used to measure inaccuracies resulting from using sample data to estimate population characteristics, i.e., sampling error. Because US-VISIT's ADIS records contain population data—rather than data based on a sample—significance tests have not been necessary in calculating overstay rates.

Rather than sampling error, a much larger issue in estimating overstay rates is non-sampling error, such as data quality issues. DHS is working to address the departure matching issues through the enhancement of its existing biographic exit program where carrier data is provided to DHS via U.S. Custom and Border Protection's Advance Passenger Information System (APIS) program, and then recorded into the Arrival and Departure Information System (ADIS). This enhancement also includes improvements to APIS and ADIS. The system improvements will allow DHS to more readily determine if there are deficiencies in data provided by the airlines, provide better matching of biographic records while maximizing the chances of automated matches, and reduce the need for costly manual reviews.

67123.198

Question#:	6
Topic:	overstay rate 2
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Please provide the Committee with the overstay rates for all nationalities and visa classes admitted into the United States in FY2010 and to date in FY2011.

Response: The Department of Homeland Security (DHS) is currently collecting the overstay data for Fiscal Year (FY) 2011. At this time, the Department cannot provide overstay rates for all nationalities and visa classes admitted into the United States in FY 2010 and to date in FY 2011. DHS will be able to provide statistical significant statistics in nine months to one year.

Question: Please provide the Committee with data concerning how many potential overstays were referred to ICE by US-VISIT in FY 2010 and FY 2011 to date, including a detailed analysis of how these cases were ultimately resolved (i.e., what percentage were found to have left, changed status, were ultimately apprehended, or were confirmed as an overstay but never found).

Response:

US-VISIT Referrals to U.S. Immigration and Customs Enforcement (ICE) Fiscal Years 2010-2011

ICE Action on US-VISIT Referral	Reason/Outcome for ICE Action		FY 2010		FY 2011	
Closed	Departure		3,519		3,664	
	Adjustment of status		4,758		1,221	
	Other reasons[1]		16,921		28,041	
Leads requiring analysis by ICE Homeland Security Investigations	Leads with unknown location[2]		2,511		10,762	
	Total investigations initiated	Total Arrests[3]	267	2,492	4	496
		Subject Departed	817		37	
		Subject Adjusted Status	218		9	
		Unable to Locate	516		30	
		Open in the Field	674		416	
Total number of leads imported from US-VISIT[4]			**30,406**		**48,366**	

[1] Other reasons include leads that do not meet national security criteria.
[2] ProMonitor is a commercial monitoring service utilized by the Counterterrorism and Criminal Exploitation Unit (CTCEU) to assist in locating subjects with an unknown location.
[3] The total number of arrests is the result of investigations that have been initiated in the fiscal year.
[4] US-VISIT provides overstay files to CTCEU on a weekly basis. The CTCEU only imports files for which it does not already have a pending or open case. Includes minors and non-priority records

67123.199

Question#:	7
Topic:	NSEERS program
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: DHS recently announced the end of the NSEERS program. It is the Committee's understanding that US-VISIT will now take over the responsibility for identifying potential overstays for individuals who were previously subject to NSEERS. However, the NSEERS program identified potential overstays on the first day their legal status expired, while the Committee's understanding is that US-VISIT program uses a different timetable for identifying potential overstays.

Please explain for the Committee how the transition from NSEERS to US-VISIT will take place.

Will US-VISIT provide ICE with potential overstay leads for individuals who would have been required to register with NSEERS as soon as they overstay the terms of their admission?

Response: It has always been the responsibility of US-VISIT to identify potential overstays. This has been true for several years even while the NSEERS program was in effect. NSEERS dealt only with certain nationalities, and DHS sought to have a biographic exit program that covered all foreign nationals. Overstays for DHS are defined as individuals who have overstayed their period of admission in the United States.

US-VISIT reviews in-country overstay records using the following priority:

1. National Security/Public Safety/Rules based Threat Records
2. Overstay records originating from Priority Countries of Interest
3. Visa Waiver overstay violators
4. Non-priority country overstay records who arrived in a specified geographic area
5. Remaining non-priority records.

In addition the DHS biographic exit program provides evidence for sanctions against those who overstay and thus violate immigration law: persons are deemed inadmissible and placed on overstay watchlists, visas are cancelled, and other actions are taken. The proposed enhancements to our existing biographic exit program are as follows:

d) Reviewing and eliminating the existing unvetted overstay records: As of May 2011, there were 1.6 million biographic records where a departure was not matched to an arrival record indicating a possible overstay, as the GAO report noted. Through a new automated review process, comparing these records to ADIS and the USCIS

67123.200

Question#:	7
Topic:	NSEERS program
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Computer Linked Application Information Management System (CLAIMS), 863,000 records are no longer considered potential overstays through information discovered from those systems. The remaining 757,000 records require a manual review to determine if the record is truly an overstay, or if the traveler actually has, in fact, departed or lawfully extended his or her status. A full review of outstanding overstay records will ensure all records checked against the Department's targeting rules and also establish a country-by-country overstay rate with high fidelity.

e) Matching all overstay records against CBP's targeting rules: As discussed above, the automated and manual reviews against CBP's targeting rules are ongoing, and from a security standpoint, will enable DHS to take action against those who have overstayed within priority enforcement areas. All overstay records are vetted against the holdings of the National Counterterrorism Center (NCTC) and others in the Intelligence Community.

f) Technical Enhancements to CBP's APIS and NPPD's ADIS systems: The APIS system enhancements will allow DHS to more readily determine if there are deficiencies in data provided by the airlines. APIS will utilize interactive communications to alert air carriers when the APIS information provided is unable to be validated against source information held by DHS such as a Lawful Permanent Resident card, non-immigrant visa, ESTA or US-issued passport. Validation will occur for both arrival and departure manifest submissions, allowing for better matching of biographic records while maximizing the chances of automated matches, negating the need for more costly manual reviews in the future. ADIS enhancements will include better and faster access to immigration benefit data held by USCIS, which will increase the accuracy of identifying overstays in an automated way, reducing the cost and time of reviewing cases manually.

This biographic exit program has been functional for many years, and was recently enhanced through changes to the Advance Passenger Information System (APIS) that took place in 2007. APIS is the system that air carriers use to report passenger manifests to DHS, and is used to match to existing information on foreign nationals who have previously entered the United States.

Overstays are identified using the APIS/ADIS systems from the time the person is identified as not having departed as of the time their lawful period of admission expires. The biographic exit program provides leads to ICE based on priority of risk to public safety. Pursuant to existing statutes, any overstay results in the automatic cancellation of the person's visa, if any, and ESTA approvals, and the inability of the person to use the

67123.201

Question#:	7
Topic:	NSEERS program
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Visa Waiver program (VWP) ever again. If the overstay period is beyond 180 days but less than 1 year, the person is statutorily inadmissible for a period of three years; if the overstay period is more than one year, the inadmissibility period is ten years. In these cases, the person could not lawfully be admitted to the United States without a waiver. In addition, at any time beyond a person's lawful period of authorized stay, that person is subject to removal from the United States and not lawfully permitted to work.

DHS is currently developing and piloting ways in which to use CBP, ICE, and US-VISIT's resources to fully automate the process of identifying overstays. See earlier sections of this response. This will allow ICE to get its leads faster and more effectively, and ensure that DHS can check all overstay records in a timely manner.

Question#:	8
Topic:	share
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: This Committee strengthened the security of the Visa Waiver Program in 2007 by requiring that participating nations enter into information sharing agreements with the United States. Specifically, DHS has interpreted this provision as requiring nations to share biometric law enforcement information and terrorist watchlist information. Mr. Heyman testified before the committee in December, 2009 that DHS was close to implementing the first electronic biometric law enforcement sharing agreement. And yet a recent GAO report found that we have only signed these agreements with barely half of the Visa Waiver nations, and that none of these agreements have actually been implemented to date. This means that we are missing an important opportunity to share real-time biometric information on serious criminals—including terrorists—with our partners abroad.

Please provide the Committee with a detailed explanation for why the implementation of these agreements has been so delayed.

When we will actually implement these agreements?

It is vitally important that border officials be notified in a timely manner of fingerprint matches with criminal or terrorist records. Are these international agreements being structured and implemented in such a way as to ensure that fingerprint matching can be done in seconds, rather than minutes or days?

Response: The *Implementing Recommendations of the 9/11 Commission Act of 2007* (Pub. L. No. 110-53) (9/11 Act) requires that Visa Waiver Program countries "enter into an agreement with the United States to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States and its citizens." DHS and its interagency partners have determined that this requirement can be fulfilled through the completion of the Homeland Security Presidential Directive Six (HSPD-6) arrangement to share information on known and suspected terrorists, and a Preventing and Combating Serious Crime (PCSC) agreement to share information on suspected criminals.

The Federal Bureau of Investigation's Terrorist Screening Center implements the HSPD-6 arrangement, the details of which are classified. Nineteen of the thirty-six VWP countries have signed HSPD-6 arrangements, and exchanges of information have taken place with almost all of these countries. The State Department and the Terrorist

67123.203

Question#:	8
Topic:	share
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Screening Center may provide further information on negotiation and implementation of the HSPD-6 arrangement.

As of August 2011, nineteen of the thirty-six VWP countries either have signed the PCSC agreement or (in one case) were deemed to have equivalent mechanisms for information exchange under previous arrangements. Four additional countries have agreed to final texts – those agreements are currently being translated in anticipation of signature in the coming months. Negotiations are ongoing with several more countries, and DHS expects to complete additional agreements by the end of the year.

Implementation of the PCSC agreements is complex, and several factors have contributed to delays in full implementation. Many of the signed PCSC agreements require ratification by foreign parliaments before information can be exchanged. Additionally, DHS and the FBI are working through a series of technical challenges which will take some time to resolve.

The U.S. government is working with the remaining countries to complete requirements in line with their biennial review of continuing VWP eligibility.

Biometric information on potential criminals and terrorists is already being shared with VWP partners on a daily basis through existing law enforcement channels and international agreements. The PCSC agreement will streamline these existing exchanges, allowing for a greater volume of queries and a rapid, automated response when a party submits a query to the other party's fingerprint database. Yet even without implementation of the PCSC's agreement's automated exchange mechanism, information is already being exchanged on a "real time" basis through our strong relationships with VWP partners.

Question#:	9
Topic:	consular posts
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Committee continues to be disappointed that there are no current plans for expanding the Visa Security Program to the 57 high risk consular posts that have been identified by the Department of Homeland Security and the Department of State. A recent GAO report found a number of problems with the program's implementation.

Please explain to the Committee what the Department's goals are for this program, and why there is no funding in the FY2012 request for continuing its expansion.

Please explain to the Committee how DHS plans to address the various implementation issues raised by the GAO in its report.

****Law Enforcement Sensitive – For Official Use Only****

Response: REDACTED.

****Law Enforcement Sensitive – For Official Use Only****

Question#:	10
Topic:	agreement
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Committee understands that DHS has reached agreement with the European Commission on a draft Passenger Name Records Agreement, but that this agreement must be ratified by the European Council and the European Parliament.

What is DHS' contingency plan should the PNR agreement fail to be ratified to ensure that we continue to receive PNR data?

Has DHS considered negotiating PNR agreements bilaterally, or requiring PNR agreements for participation in the Visa Waiver Program?

Response: The ratification of a Passenger Name Record (PNR) agreement is extremely important to the European Union, not only for bilateral relations but for their own purposes including: advancing a PNR system in Europe; providing legal certainty for the airlines; and protecting the traveling public. As such, the Department continues to believe that it is unlikely that the European Commission would advance an agreement to the European Parliament that would fail to be ratified. Until then, the 2007 agreement remains provisionally in effect.

Even if the 2007 agreement was not in effect, or if the new agreement failed to be ratified, the Aviation and Transportation Security Act of 2001 and the Department of Homeland Security (DHS) regulations require carriers to make PNR data available if they collect it. In short, failure to ratify the agreement would not change U.S. law, regulations, or requirements. In order to transport passengers to the United States, carriers will still be required to provide the U.S. Customs and Border Protection with access to PNR data if they collect it.

After the entry into force of the EU's Lisbon Treaty on December 1, 2009, European institutions are determining how they negotiate and reach agreements with third parties. The Department of Homeland Security (DHS) and the European Union signed the agreement on December 14, 2011. Only Parliamentary consent remains to be achieved before the agreement can enter into force. At this point, the Department continues to believe that considering alternative pathways to achieving legal certainty and a new PNR arrangement is premature. Our European partners have stated that the current draft Agreement is a significant improvement to the 2007 Agreement. DHS remains confident that we will reach an agreement.

67123.206

Question#:	11
Topic:	counterterrorism
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Mr. Beers focused part of his testimony on his role as DHS Coordinator for Counterterrorism, as designated in March 2010 by Secretary Napolitano.

This position and any related office are not codified in statute. The 2010 DHS Bottom Up Review noted that the Department would "continue to evolve the Counterterrorism coordination function in consultation with Congress." Has the Department developed a proposal for the long-term role and responsibilities of the Counterterrorism Coordinator, and if so, what is it?

Mr. Beers' testimony notes that his key role is to "improve coordination among the operational components and to bring together the policy and intelligence components to support this effort." How is this role distinct from the role of the DHS Office of Operations Coordination, which (according to the Department's website) is responsible for "conducting joint operations across all organizational elements"?

How many individuals currently are working in support of the Coordinator for Counterterrorism? From what DHS office or directorate's budget are their positions funded? Please provide a detailed breakdown of personnel and funding.

Question: This position and any related office are not codified in statute. The 2010 DHS Bottom Up Review noted that the Department would "continue to evolve the Counterterrorism coordination function in consultation with Congress." Has the Department developed a proposal for the long-term role and responsibilities of the Counterterrorism Coordinator, and if so, what is it?

Response: As part of the Department of Homeland Security's (DHS) Bottom-Up Review in July 2010, the Department concluded that "Although DHS is one of the Federal Government's key counterterrorism agencies, DHS did not have a single coordinating entity for counterterrorism activities" prior to naming Under Secretary Beers to the Counterterrorism (CT) Coordinator role.[1] Following the failed cargo plots of October 2010, Secretary Napolitano took the added measure of authorizing the creation of a Counterterrorism Advisory Board (CTAB), which consists of leadership from across DHS's Operational Components, and is overseen by the CT Coordinator. The Advisory Board's evolution into a trusted forum for cross-Component coordination and planning

[1] Bottom-Up Review Report, U.S. Department of Homeland Security, July 2010, p. 8.

67123.207

Question#:	11
Topic:	counterterrorism
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

was recognized in April 2011, when Secretary Napolitano signed the CTAB Charter, which formalized the mission of the CTAB and affirmed the leadership of the CT Coordinator.

At the recommendation of the Deputy Secretary, the Department also established a working group to support the CT Coordinator. The Counterterrorism Working Group (CTWG) consists of members either detailed from DHS Components or assigned to it as an additional duty. The Principal Deputy CT Coordinator is detailed from the DHS Office of Intelligence and Analysis and has the day-to-day responsibility of managing the working group and overseeing CT issues.

The Department has increased planning for the maturation and long-term role and responsibilities of the CT Coordinator and has also strengthened coordination and improved staff support for the position. DHS also briefed relevant congressional committees regarding the current structure of this position and has discussed other, similar models for coordination with the Homeland Security Institute. The Department looks forward to working with your committee to mature the coordination function over the next year.

Question: Mr. Beers' testimony notes that his key role is to "improve coordination among the operational components and to bring together the policy and intelligence components to support this effort." How is this role distinct from the role of the DHS Office of Operations Coordination, which (according to the Department's website) is responsible for "conducting joint operations across all organizational elements"?

Response: The CT Coordinator is responsible for the coordination of all DHS activities across the counterterrorism enterprise, which extends beyond the joint-operations and reporting activities overseen by the Office of Operations Coordination (OPS). CT coordination includes syncing intelligence with operators in relevant Components, breaking down obstacles that prevent Components from responding to threats with appropriate countermeasures, identifying systemic challenges affecting the Department for referral to the DHS Office of Policy, and other responsibilities. The CT Coordinator accomplishes this coordination through the CTAB in leveraging the unique authorities and responsibilities of the DHS components.

The DHS CT Coordinator's singular focus on the Department's primary mission—preventing a terrorist attack—further differentiates it from OPS, which plans joint-operations for a range of departmental missions and is not singularly focused on the Department's first mission.

67123.208

Question#:	11
Topic:	counterterrorism
Hearing:	Ten Years After 9/11: Preventing Terrorist Travel
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Finally, the CT Coordinator also oversees the CTAB, the only forum for high-level, counterterrorism coordination across all of DHS.

Question: How many individuals currently are working in support of the Coordinator for Counterterrorism? From what DHS office or directorate's budget are their positions funded? Please provide a detailed breakdown of personnel and funding.

Response: The CT Coordinator and the CTWG do not have an independent operating budget. Secretary Napolitano assigned Under Secretary Beers to his role as CT Coordinator as an additional duty. The CTWG has 10 members that are either detailed from Components or assigned to it as an additional duty. The Principal Deputy CT Coordinator is detailed from the Office of Intelligence and Analysis and has day-to-day responsibility for managing the working group and overseeing CT issues.

The National Protection and Programs Directorate funds three members of the CTWG in addition to Under Secretary Beers, and the Office of Intelligence Analysis funds two CTWG members in addition to the Principal Deputy CT Coordinator. The DHS Office of the Secretary, the Office of Operations Coordination, Office of Intergovernmental Affairs, and Transportation Security Administration each fund one member of the CT Working Group. Other offices and components support the work of the CTAB and the CT Coordinator in addition to those that form the working group. Individual Components are responsible for all costs, including information technology systems, office supplies, benefits, and any travel for their representative members.

67123.209

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#1)
Senate Committee on Homeland Security
July 13, 2011

Question:

A recent GAO report highlighted some significant issues with the implementation of the Visa Security Program. GAO found disagreements between consular officers and ICE agents at some posts concerning how close an association with terrorism was needed to deny someone a visa.

Can you explain for the Committee exactly what kind of association with terrorism would be considered significant enough by the State Department to bar someone from being issued a visa?

Answer:

To find someone ineligible for a visa for association with terrorism, a consular officer would have to know, or have reasonable ground to believe, that a visa applicant has engaged, or is likely to engage, in any of the terrorist activities defined in Section 212(a)(3)(B) of the Immigration and Nationality Act (INA), which include actual participation in a terrorist activity, as well as membership in a terrorist organization, endorsing or espousing terrorism, providing material support to a terrorist organization, and related activities. The interagency Security Advisory Opinion process is the mechanism used by the Department of State to provide consular officers advice and background information to adjudicate visa

67123.210

applications of visa applicants with confirmed or suspected links to terrorist activities.

The "reasonable ground to believe" standard, which must be met to sustain a finding of inadmissibility under INA 212(a)(3)(B), is higher than the standard for watchlisting: a "reasonable suspicion" that the individual is a known or suspected terrorist. In most instances, information that resulted in watchlisting an individual will also be considered sufficient to sustain a finding of inadmissibility under INA 212(a)(3)(B), should the watchlisted individual apply for a visa. On rare occasions, however, State Department analysts conclude that either the derogatory information or the identity information available to the U.S. government is insufficient to sustain a finding of inadmissibility for terrorist activity in a particular visa case. The same law and standards govern DHS adjudications of individuals seeking admission into the United States.

Regarding cases in which derogatory information is insufficient to sustain terrorism ineligibilities, in 2010 the Department reiterated its guidance to consular officers on the use of their discretionary authority to deny visas under section 214(b) of the Immigration and Nationality Act, with specific reference to cases that raise security and other concerns. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

67123.211

Question:

Under what circumstances might a consular officer disagree with an ICE agent on this issue, and what are the mechanisms for resolving these disagreements?

Answer:

The few disagreements that arise concern differing interpretations of the INA. Given the volumes of information that consular officers and their ICE/VSU colleagues are reviewing, and the differences in background and experience they bring to the process, occasional disagreements do arise as reasonable and conscientious professionals consider the same set of facts and reach different conclusions. As with any process involving so many records and individual travelers, a small number of adjudications require extra effort to complete, a process facilitated by the positive working relationships among interagency partners.

In January 2011 the State Department Bureaus of Consular Affairs and Diplomatic Security and the Department of Homeland Security, U.S. Immigration and Customs Enforcement, concluded a Memorandum of Understanding on Roles, Responsibilities, and Collaboration at Visa Security Units Abroad. Among other provisions, a dispute resolution section implements the provisions of Section 6(f)(2) of the Memorandum of Understanding between the Secretary of State and

67123.212

the Secretary of Homeland Security Concerning Implementation of Section 428 of the Homeland Security Act of 2002 (dated September 26, 2003).

Accordingly, in cases in which Visa Section personnel and the VSP agent at post disagree on the refusal or revocation of a visa, the dispute will be raised to the Consular Section Chief and Senior ICE Agent at post. If the Consular Section Chief and the Senior ICE Agent cannot agree at post, an SAO or Advisory Opinion cable is to be transmitted to the State Department and to ICE Homeland Security Investigations (HSI) International Affairs (IA), for resolution in Washington. No visa can be issued while the case is under review in Washington.

67123.213

Question:

During her testimony, Assistant Secretary Jacobs noted that these kinds of disagreements were rare. How many instances of such a disagreement have occurred in the past year? In the past five years?

Answer:

These disagreements are so rare that neither the Department of State nor the Department of Homeland Security collects statistics. Since the signing of the MOU in January 2011 no cases have required formal dispute resolution in Washington.

In the five previous years, while a small number of cases were the subjects of communications between posts and our respective headquarters, no formal dispute resolution meetings were held between State and the ICE Visa Security Program.

67123.214

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#2)
Senate Committee on Homeland Security
July 13, 2011

Question:

DHS and the State Department identified 57 consular posts that were deemed high-risk as part of their collaboration over the Visa Security Program. While this analysis was done specifically in the context of expanding the VSP, giving consular posts specific risk-ratings appears to provide valuable information that could be used by the State Department in order to inform its consular activities and deployments.

Please provide the Committee with a detailed explanation of what went into this assessment. What factors would result in a consular post being designated as high risk?

Answer:

The Department of Homeland Security, with the advice and participation of the Department of State as well as the federal law enforcement and intelligence community, considered a number of factors, including those listed below, to determine the list of high-risk posts:

- An Intelligence Community threat assessment of political violence, indigenous terrorism, transnational terrorism, and other factors.

- National Security Records of known or suspected terrorists (KSTs), sorted by place of birth, assessed by the Terrorist Screening Center.

67123.215

- Applications requiring an SAO, sorted by post. Related to that, the number of "SAO Positives," which measures the number of positive matches to U.S. government databases, sorted by the U.S. embassies or consulates where the visa application was processed.

- ICE administrative arrests, sorted by the nationality of aliens subject to administrative arrests.

- National Security arrests (criminal and administrative) and National Security investigations opened by ICE during the specific time frame considered.

- Volume of visa activity, including refusal, revocation and SAO volumes, derived from State Department's Consular Consolidated Database.

- Level of country corruption.

- The number of nonimmigrant visas cancelled at U.S. Ports of Entries, compiled by Customs and Border Protection.

67123.216

Question:

Does the State Department incorporate risk assessments into its operations? If so, please provide detailed information about how this takes place. If not, what is the rationale for not incorporating risk assessments into consular operations?

Answer:

We provide the same high level of security and screening of all visa applications, regardless of the level of risk assigned by the interagency process to a particular consular post. All visa applications are adjudicated according to the law, taking into account the circumstances of the alien as well as any information made available by any of the relevant U.S. government agencies at the time of the visa application. Applicants' names and biometric data are run against DHS's Automated Biometric Identification System (IDENT), the FBI's Integrated Automated Fingerprint Identification System (IAFIS), and facial recognition software, as well as against the Consular Lookout and Support System (CLASS), which contains data provided to the State Department from law enforcement and intelligence databases. Regulations pertaining to the Advisory Opinion and Security Advisory Opinion processes are uniform across all of our consular posts. Consular officers at all posts receive briefings and work cooperatively with political, economic, security, and other colleagues at post to ensure wide dissemination of threat and other information.

67123.217

Consular officers receive professional development training as well as post-specific training throughout their careers. We continually update training for new and experienced consular officers on the latest technology, foreign language, fraud prevention, and interviewing skills. Required regular post reporting is used to identify fraud trends and address any potential vulnerabilities in the visa process.

67123.218

Question:

Please explain to the Committee what special training or instruction is given to consular officers who are deployed to work at high-risk consular posts?

Answer:

All officers devoted to visa adjudication are highly-qualified, well-trained, and motivated professionals committed to a career serving the United States overseas. Training gives these consular officers particular expertise in identifying individuals who possess fraudulent documents, are imposters, or are otherwise attempting to enter the United States improperly. High-risk applicants can, and do, apply at any visa-issuing post in the world, whether it is considered a high-risk post or not. All consular officers, regardless of where they serve, are prepared to adjudicate high-risk cases.

Consular training at the Foreign Service Institute begins with the Basic Consular Course – an intensive 31-day curriculum that provides an in-depth focus on security-related training. Subjects covered include recognizing and combating fraud as well as terrorist mobility and alien smuggling, with close to 40 classroom hours incorporated on themes related to Security, Accountability, Fraud, and Ethics.

Officers then receive continuing education on these themes throughout their careers, including courses in fraud prevention, advanced security name-checking,

67123.219

and an in-depth exposure to interviewing techniques designed to help them recognize cognitive and emotional micro-expression clues from an applicant.

In addition, officers en route to posts abroad receive targeted area studies courses to familiarize them with the unique historical, cultural, and political contexts that will have an impact on consular decision-making. They also have consultations with the Visa Office and other Consular Affairs offices. Officers assigned to certain high-risk posts also receive advanced defensive driving, firearms and explosives familiarization courses, and other specialized training.

67123.220

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#3)
Senate Committee on Homeland Security
July 13, 2011

Question:

The United States is one of the few countries in the world that does not feature a separate consular career track for all consular officers; instead all Foreign Service officers must spend one deployment working as consular officers. There is some concern within the Committee that deploying junior Foreign Service officers to high-risk posts may represent a weakness in our efforts to prevent terrorists from traveling.

Has the State Department at any time considered sending more senior consular officers to work at high-risk consular posts?

Answer:

The State Department does send its most experienced and talented officers to our most challenging posts. Serving well at these posts is rewarded in our personnel system, so our best officers apply. At the same time, high risk applicants can and do apply at every post, and all consular officers are fully trained and have the resources to detect threats wherever they are serving. After September 11th, we worked with Congress and our interagency partners to implement a host of new security measures, including increased staffing at high-risk posts and greater oversight by supervisors at all posts. American consular associates and assistants may no longer adjudicate visas - only commissioned consular officers or

67123.221

Professional Adjudication Specialists with equivalent training and qualifications may do so. Supervisors are now required to review adjudications by interviewing officers daily, with compliance monitored in Washington. We developed an intensive, one-week course in advanced name-checking and interviewing techniques for all adjudicating officers, and greatly increased data sharing with law enforcement and intelligence agencies even before an applicant appears for a visa interview. In addition to enhanced name-checking software, we now apply facial recognition technology to all adult visa applicants. We regularly review circumstances at our posts worldwide, and adjust staffing levels as well as the level of experience required for the officers we assign.

Question:

What impact would such a policy change have on State Department operations?

Answer:

As noted above, the State Department does send its most talented and experienced officers to high-threat posts.

67123.222

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#4)
Senate Committee on Homeland Security
July 13, 2011

Question:

As the scrutiny of travel documents has ramped up, one area that remains troubling is the use of fraudulent breeder documents to obtain passports and other travel documents. The United States has pushed for increasing the security passports and visas around the world, but if these secure travel documents can be obtained with fraudulent source documents then we have effectively allowed terrorists access to travel documents that make them virtually immune to discovery. A number of federal agencies have programs that aim to assist other countries improve their ability to identify fraudulent documents. However, a recent GAO report concludes that our government's efforts are not being coordinated well.

How does the State Department plan to address the issues raised by the GAO report?

Answer:

A secure travel document issuance process helps border authorities determine whether an identity document is genuine and is carried by the legitimate holder. Although raising the barriers to identify document fraud will not eliminate all terrorist acts or criminal activity, it will make transnational criminal activities more difficult to undertake and increase the level of sophistication and cost required to elude detection.

67123.223

There are major challenges inherent in combating the use of fraudulent breeder documents used as the basis for obtaining a travel document – particularly the lack of international standards and the multiplicity of documents. Documents which can be used to obtain a passport can come from a variety of different levels and branches of local and national governments, each with varying security standards, and this is a problem both domestically as well as internationally. Currently in the United States there are over 14,000 variations of birth certificates in circulation.

The Department is one of many organizations that have identified the integrity of breeder and travel documents as a global concern. The Department, along with domestic and international partners, is focusing on the manner in which breeder documents are issued. Along with the Department of Homeland Security (DHS), we are assisting the development of minimum standards for birth certificates which are used for acquiring travel, residence, and identity documents. These standards would have direct consequences for the integrity of passport issuing authorities. Authorities would be able to establish with greater certainty the identity of the person applying for a travel, residence, and/or identity document. The Department, along with DHS representatives, is seeking to incorporate standardized breeder document specifications into International Civil

67123.224

Aviation Organization Document 9303, which lays out the specifications for all travel documents to ensure they are globally interoperable for international travel.

The Department continues to fund programs and provide other resources for bilateral or multilateral capacity building. The Department contributes valuable experience and insight to other issuing authorities. For example, the Bureau of Consular Affairs (CA), in close coordination with the Government Printing Office and the Department of Homeland Security, has supported over 45 foreign delegations (FY 2006-2010) in their pursuit of machine readable travel documents or improving their understanding of electronic machine readable travel documents and improving their issuing processes. Allowing others to see our adjudication process, our use of identity management tools, and our best practices articulates our focus on combating fraudulent breeder documents and our strategy in combating terrorist and criminal travel. Sharing what we know aids in the capacity building of our international partners.

CA is working with the Bureau of International Narcotics and Law Enforcement Affairs' (INL) International Law Enforcement Academy (ILEA) network to provide passport anti-fraud training to officials from foreign passport issuance agencies. The first training workshop entitled "Managing an Effective Passport Integrity and Anti-Fraud Program," will be piloted in September 2011 in El Salvador for officials from five Central American counties. The training is

67123.225

designed to improve the integrity of other countries' passport issuance by helping them institute organizations, processes, and procedures for detecting fraudulent passport applications as part of their adjudication and issuance processes. In FY 2012, CA and INL propose to deliver two workshops, one in Africa for English-speaking African nations and one in San Salvador for Spanish-speaking Caribbean nations.

In April 2011, CA greatly enhanced the way it tracks visa fraud. It deployed globally a tool called the Enterprise Case Assessment Service that provides a platform to store fraud-related research that used to be stored, for the most part, outside of consular systems. This new tool associates fraud-related information with visa records, making it available to consular officials around the world. Should fraud be confirmed during the course of a visa interview, consular officers can record that data in this new tool, where it can be easily referenced if the individual attempts to re-apply. Future iterations of this tool will track fraud in other consular services, such as U.S. passport applications, and will enable CA to track the activities of third-party document vendors and visa fixers. While respecting privacy concerns, CA is exploring the possibility of sharing this new data source with its U.S. government partners to enhance interagency cooperation on fraud prevention.

67123.226

As threats to U.S. security have risen and spread in the past decade, CA has renewed its commitment to enhanced information sharing and analysis with interagency and international partners by, among other efforts, sharing lost and stolen passport data with the International Criminal Police Organization (INTERPOL), developing a workshop for foreign government passport-issuing officials on establishing an effective fraud prevention program, and presenting on travel document security at the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex) Security Document Workshop. A CA representative is scheduled to attend a Frontex meeting in September 2011, at which the consular anti-fraud training program Frontex is developing will be finalized.

We have taken on board the GAO's conclusion that there is a need to improve the coordination of training efforts, and are conducting sufficient training for the lessons to sink in and the message to reach all members of a partnering organization. Overseas, much training is done at little or no cost by officers already stationed in the country.

The Department along with our USG partners will continue our coordinated participation in international fora that deal with travel document security, standards, issuing processes, and information data sharing. Some of the specific functions we will coordinate on are: supporting foreign delegations in their pursuit

67123.227

of machine readable travel documents; participation with our international partners such as the International Civil Aviation Organization, the European Union, Interpol, the G-8, the Asian-Pacific Economic Cooperative, and the Organization for Security and Cooperation in Europe; supporting the Five Nations Liaison and other international exchanges; and, improving bilateral assistance and cooperation.

67123.228

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#5)
Senate Committee on Homeland Security
July 13, 2011

Question:

In staff briefings, the GAO noted that the State Department has a number of programs dealing with terrorist travel issues that are dispersed throughout the Department and that are largely not coordinated. How will the State Department ensure that it is effectively coordinating its own efforts to help foreign partners develop terrorist travel programs?

Answer:

The Department of State's Office of the Coordinator for Counterterrorism (S/CT) leads the Department and the U.S. Government on international counterterrorism (CT) issues and programs, working closely with State's bureaus and offices, DHS, the National Counterterrorism Center (NCTC), the FBI, and the intelligence community. S/CT plays an interagency coordinating role for CT and homeland security issues that cut across the whole State Department.

S/CT regularly engages our foreign partners bilaterally, regionally, and on a multilateral basis to address the global issue of terrorist transit. We work in close coordination with State bureaus and offices and the interagency community to develop and implement a full range of counterterrorism programming. In particular, we emphasize the importance of regional programming. Stronger

67123.229

regional cooperation across borders makes it more difficult for terrorists to move freely.

In Washington, S/CT participates in regular National Security Council-led meetings, as well as meetings organized by other agencies, including Department of Defense and the NCTC, to coordinate our policies in countries and regions that pose terrorist threats. In addition, State organizes regular meetings with our interagency colleagues and other State bureaus to exchange information and coordinate our activities with our foreign partners on a bilateral and regional basis. Programs to prevent terrorist travel figure prominently in these regular discussions.

In the field, S/CT runs the Regional Security Initiative (RSI), which brings together our Embassy leadership with senior interagency representatives to provide a strategic focus to our capacity building efforts in critical regions of the world. We have posted S/CT field officers in six locations (Nairobi, Kuala Lumpur, New Delhi, Athens, Ankara, and Algiers), each of whom travels regularly to all of the posts in his or her region to coordinate programs and policies, in addition to maintaining frequent electronic contact.

S/CT coordinates several S/CT-specific activities to combat terrorist travel with the appropriate State bureaus and offices, including administering the Anti Terrorism Assistance (ATA) program with the Bureau of Diplomatic Security

67123.230

(DS), which includes training in the detection of fraudulent travel documents, as well as broader courses in airport and aviation security, port security, and border management. As part of the ATA program, teams from S/CT and DS visit our partner countries every two years to assess holistically the situation at all levels, from policy and strategy to implementation and operations. These assessments cover a wide range of factors, including the host country's political will and cooperation, program effectiveness, outcomes of previously provided assistance, progress toward the achievement of objectives, and sustainability. ATA assessments also evaluate the technical and institutional capabilities of the host country to detect and counter terrorists and, if applicable, recommend possible further USG assistance. The results of these assessments are shared with the appropriate State bureaus and offices and our interagency partners to facilitate coordination.

S/CT helps foreign partners create their own computerized database systems with terrorist screening information, under the TIP/PISCES program (Terrorist Interdiction Program / Personal Identification Secure Comparison and Evaluation System). S/CT leads HSPD-6 negotiations with foreign partners to share terrorist screening information, with the support of the Terrorist Screening Center (TSC). In addition, S/CT works with DHS to negotiate agreements with foreign partners to share Advance Passenger Information (API) and Passenger Name Record (PNR)

67123.231

data. Most notably, State and DHS are currently negotiating a PNR agreement with the European Union (EU) to replace the 2007 agreement that is in force provisionally.

Finally, S/CT and the DHS Office of International Affairs are co-chairing a new Interagency Working Group on Aviation Security Assistance overseas. The purpose of the IWG is to offer strategic coordination among the many USG agencies and programs that address aviation security assistance. This group, which includes a number of State bureaus and offices, will be a forum for information-sharing, transparency and de-confliction.

In an additional effort to enhance coordination, the Office of Consular Support in the Bureau of Intelligence and Research accesses highly classified reports from all elements of the Intelligence Community (IC), and forwards appropriate information to consular officers abroad for appropriate action. A recent Bureau of Consular Affairs (CA) effort vastly increased the number of consular officers in key positions abroad with enhanced security clearances, enabling these officers to read more information from the IC at post, and discuss details about potential threats with their IC colleagues. CA views these enhancements to the flow of classified information from the IC to consular officers abroad as essential to stopping terrorist travel.

67123.232

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#6)
Senate Committee on Homeland Security
July 13, 2011

Question:

Please provide the Committee with a detailed explanation of how the PISCES program works, including how much has been spent on the program, what countries it operates in, what the current plans are for expanding it, and what information sharing requirements may form part of the program.

Answer:

The Terrorist Interdiction Program (TIP) seeks to constrain terrorist mobility globally by helping countries at risk of terrorist activity enhance their border security capabilities. TIP provides participating countries with a computerized watchlisting system known as PISCES (*Personal Identification Secure Comparison and Evaluation System*). Countries are identified for eligibility to participate in TIP based on known terrorist activity or transit, need for a watchlisting system, and political will to cooperate.

TIP installs PISCES hardware and software at selected points of entry in consultation with the host government, usually including international airports and major border crossings. The hardware includes commercial off-the-shelf computer workstations, passport readers, cameras, flatbed scanners, and fingerprint readers. PISCES software may be customized to meet host nation requirements. TIP also

67123.233

provides a high-speed secure connection from the host nation's centralized database, located in the appropriate government agency, to points of entry where PISCES is installed. The system enables host nation border control officials to identify suspect travelers against a current host nation maintained watchlist. PISCES is installed at both arrival and departure terminals so that host nation officials can identify travelers entering and leaving the country. PISCES enables immigration officials to use the system to collect, compare and analyze data for investigative purposes. TIP also trains host nation border control officials to operate the PISCES system and provides periodic maintenance and upgrading as necessary.

TIP/PISCES is currently operational in the following countries: Afghanistan, Cambodia, Cote D'Ivoire, Djibouti, Ethiopia, Ghana, Iraq, Kenya, Kosovo, Macedonia, Malta, Pakistan, Tanzania, Thailand, Uganda, Yemen and Zambia.

Since TIP'S inception in FY 2000 through FY 2010, the State Department has spent a total of $130.6 million on the program. A significant portion of this total spending (approximately $45 million to date) has involved the research, development, and deployment of enhanced biometrics capabilities. Beginning with the successful pilot program in Nairobi, Kenya in April 2010, the TIP program has deployed enhanced biometrics capabilities (a ten-print enrollment and

67123.234

comparison system similar to that used by US-VISIT) in PISCES countries, with the goal of providing this capability to current PISCES countries and any new countries that may join the program, subject to host nation acceptance and fiscal constraints. The enhanced biometrics capability over time will exponentially increase host nation capabilities to identify and detect terrorists traveling with fraudulent documents and alias identities. TIP program managers actively seek to expand the PISCES system to a select group of new countries based on their CT priority, need for a state-of-the-art border control system, and political will to cooperate with the United States on counterterrorism issues.

A PISCES program is generally established in a country through a Memorandum of Intentions (MOI) signed by the U.S. Ambassador or his/her designee and the appropriate host nation official in charge of border security matters. The MOI stipulates that both sides intend to exchange PISCES information and data, including travel of suspected and known terrorists.

67123.235

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Ten Years After 9/11: Improving Emergency Communications
Homeland Security and Governmental Affairs Committee
Chairman Joseph Lieberman
July 27, 2011

Good morning. This is another in a series of hearings that Senator Collins and I have been doing as we approach the 10th anniversary of 9-11 to essentially evaluate what lessons we learned from that tragic day and what we've done to act on those lessons. One of the revelations of that day was the enormous gaps in our emergency communications abilities. A lot of first responders couldn't coordinate their rescue efforts because they couldn't talk to each other.

As one New York City fire chief told the 9-11 Commission: "People watching on TV certainly had more knowledge of what was happening a hundred floors above us than we did in the lobby [of the World Trade Center]."

That proved fatal because many firefighters inside the Twin Towers didn't hear the call to evacuate.

In its report, the 9-11 Commission said:

"The inability to communicate was a critical problem at the World Trade Center, Pentagon and Somerset County Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem."

As a result, the 9-11 Commission recommended the federal government take the lead in helping state and local governments establish interoperable communications systems.

A year after the Commission issued its report, Hurricane Katrina slammed into the Gulf Coast. We saw again the relevance of the 9-11 Commission recommendation - not in relation to man-made attacks, but to natural disasters as well. In the Gulf Coast, as a result of Katrina, the lack of interoperable communications was compounded by an inability of many communications systems to operate at all under those circumstances.

Phone lines, cell towers, and electrical systems were destroyed by the storm, knocking many communication systems offline, making it impossible at times for many first responders and government officials on the Gulf Coast to talk to each other.

Mississippi Governor Haley Barbour memorably said: "My head of the National Guard might as well have been a Civil War general . . . because he could only find out what [was] going on by sending somebody."

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.236

Today, at this hearing, we're going to assess what progress we've made and what gaps remain in making public safety communications more interoperable in a crisis.

In assessing what's happened since 9-11, it's important to remember that planning and funding decisions for emergency communications traditionally have been splintered across over 55,000 public safety organizations across our country that operate on many different bands of radio spectrum.

But as we look back over almost 10 years, we have made significant progress in bringing these varied organizations together.

The "Implementing Recommendations of the 9/11 Commission Act of 2007," the second wave of legislation from the 9-11 Commission report, and written by the Committee, created the Office of Emergency Communications – or OEC – within the Department of Homeland Security (DHS) to coordinate with state and local governments in addressing the many challenges that come with trying to create interoperable communications systems.

With assistance from the OEC, each state and territory has now created a communications interoperability plan and has appointed a state interoperability coordinator. I'm pleased to say these officials meet face-to-face twice a year and are in ongoing communication about how to improve interoperability.

That's very significant because a few years ago, it wasn't always clear who was the point person in each State was for interoperability, or if there actually was such a point person.

In 2008, OEC issued the National Emergency Communications Plan to establish clear goals for improving interoperability. And to ensure that the plan is more than just a piece of paper, OEC has been testing to see if its goals are being met. In 2010, OEC tested 60 urban areas to see if they could demonstrate that they could rapidly establish communications among agencies from all levels of government in the event of an emergency.

I'm pleased to say all 60 urban areas met the goals set by OEC.

They're now working with the States to test the capabilities of the more than 3,000 counties across the country.

Significant investments in many state and local communications systems – supplemented by over $4 billion in grant funds from the DHS – have significantly enhanced voice communications and interoperability over what they were a few years ago. It's comforting to report one of the greatest success stories comes from Louisiana, which has used state money, DHS grants, and stimulus dollars to build a single, statewide radio communications system that provides daily voice communications to more than 60,000 federal, state and local users.

This system proved its worth during the evacuation of almost two million people before Hurricane Gustav in August 2008, and again after the Deepwater Horizon oil spill when the system was the back-bone for establishing interoperable communications among the various first responders in the Gulf States.

Despite such progress in voice communications, we still have failed to fulfill the recommendation of the 9-11 Commission to set aside a portion of the radio spectrum and dedicate it to create a coast-to-coast, interoperable, digital, emergency communications network.

We have the opportunity to do that right now and we need to seize it.

Currently, public safety agencies transmit on narrow slices of non-contiguous spectrum that can't handle the kinds of large chunks of data available to the average smart phone user.

Turning over a large contiguous slice of the broadband spectrum – which is known as the D Block—to public safety would give our first responders a 21st Century communications system with equipment that could share information with any other department anywhere in the nation.

Right now, as one of my staff members put it, the average first responder doesn't have the capability of the average teenager with a smart phone. That really is unacceptable.

If we close this gap, for instance, firefighters could get digital building diagrams from the local building department so they would know the floor plan and exits before they even got to the burning building.

Paramedics could send a patient's vital signs to the emergency room, so doctors and nurses would know what they were dealing with before the patient arrived.

A police officer at the scene of a crime could take electronic fingerprints and immediately compare them to Federal, State and local databases. Or the officer who gets a partial read of a license plate could immediately tap into a database to help determine who owns the car, and whether they have outstanding warrants against them.

Senator McCain and I have sponsored legislation to set aside the D Block for first responders – the "Broadband for First Responders Act of 2011" – and we are committed to working with Senators Rockefeller and Hutchison, chairman and ranking member of the Committee on Commerce, Science, and Transportation, who have reported similar D Block legislation out of their Committee.

But I will note, Senator Reid, in his proposal to end this debt ceiling crisis, has included auction money from the spectrum as contributing to diminishing the deficit. He has allocated $7 billion of that for these purposes. For reasons that are not clear to me yet, that's $4 billion less than our legislation and we want to see what's going on with that. But all the authorizing language is in Senator Reid's proposal, so we've got the possibility of actually achieving this in the next week, and that would be great.

In this 10th year after 9-11 adopting this legislation is one of the best things we can do to show we've learned the lessons from 9-11. The bottom line is our first responders need a nationwide network giving them the most modern broadband capabilities.

67123.238

Opening Statement of
Senator Susan M. Collins

"Ten Years After 9/11: Improving Emergency Communications"

Committee on Homeland Security and Governmental Affairs
July 27, 2011

The effectiveness of emergency communications has emerged as a concern due to the failures that occurred in the wake of the 9-11 attacks and the Hurricane Katrina disaster. As both of these catastrophes demonstrated, the lack of reliable communications before, during, and after a disaster can cost lives, worsen damage, and slow response operations.

Not only did the 9-11 attacks represent a "failure of imagination" as the 9-11 Commission found, they also revealed the inadequacy of communications equipment, technology, and systems. The 9-11 Commission report cited many problems with communications among firefighters on September 11th and found that the technical failure of the fire department's radios was a "contributing factor" to the loss of firefighter lives, albeit not the primary cause.

Incredibly, when Hurricane Katrina struck in 2005, we saw many of the same problems we witnessed four years earlier in the 9-11 attacks. Emergency personnel had incompatible equipment even within the same Louisiana parish. Major communications problems arose when towers and electronic equipment were destroyed; 911 centers were rendered inoperable, and the FEMA Mobile Emergency Response Systems were overwhelmed.

A FEMA official who was in New Orleans after Katrina estimated that the lack of effective communication at the Superdome reduced FEMA's effectiveness by 90 percent.

This Committee conducted an in-depth investigation into the failed response to Hurricane Katrina and detailed the various communication failures associated with the storm. Although there are numerous examples, one of the most notable assessments that sticks in my mind came from Haley Barbour, the Governor of Mississippi. He said: "My head of the National Guard might as well have been a Civil War general for the first two or three days because he could only find out what is going on by sending somebody. He did have helicopters instead of horses, so it was a little faster, but the same sort of thing."

When seconds and minutes are important, communications systems must be both operable and interoperable so that first responders can talk to each other and coordinate their operations. We never again want to see individuals

67123.239

on rooftops pleading for help that may be delayed because of an inability of responders to communicate with one another. We must be especially sensitive to the ability to communicate with the most vulnerable in our population, such as children, the elderly, or those with special needs.

As the 10th anniversary of 9-11 approaches, how first responders communicate with one another and how Americans receive emergency information remain challenges.

Public safety officials should have access to state-of-the-art, interoperable communications equipment to use during emergencies. But we must be sure that resources are invested carefully and that an effective and efficient structure is established to manage emergency communications. Plans and systems must be tested during state, regional, and national level exercises.

Today, the Committee will examine the progress made in the last decade and explore what more needs to be done. After Katrina, Congress created the Office of Emergency Communications (OEC) within DHS, which developed a National Emergency Communications Plan, stood up Regional Working Groups, and established goals to measure progress.

The Chairman and I also created an Interoperability Emergency Communications Grant Program to support state plans. This program has supplemented other federal, state, and local investments. According to CRS, as much as $13 billion in federal funding has been spent on emergency communications during the past nine years.

What do we have to show for these investments? Are we making progress? Is the money being well spent so that we will be better prepared for the next major disaster?

My own state of Maine has done a great deal to increase the ability of first responders to communicate with each other. Notably, the State has also been working with Canada to ensure that first responders across our more than 600-mile international border can communicate with each other in an emergency.

The investments, training, new equipment, and planning have produced some successes. For example, in recent testimony, FEMA Administrator Fugate testified that interoperable communications were effectively used after the Joplin, Missouri, tornado and that the success of state and local responders reduced the burden on the federal government.

Another issue is the importance of effective communication with the public before, during, and after an incident. Much like the communication among first responders, the communication between officials and the public is vitally important and can save lives. I will soon introduce legislation on which I look forward to working with the Chairman, to strengthen the nation's public alert and warning system.

I want to welcome all of the witnesses.

67123.240

Statement for the Record
of
Greg Schaffer
Acting Deputy Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs Committee
Washington, DC

July 27, 2011

Introduction
Thank you Chairman Lieberman, Ranking Member Collins, and distinguished members of the Committee. It is a pleasure to discuss the Department of Homeland Security's (DHS) efforts to improve communications for emergency response providers and government officials. As we approach the tenth anniversary of the attacks of September 11, 2001, there is no shortage of reminders of the need for an effective and efficient emergency response framework to manage incidents and restore essential services in the aftermath of a disaster. As just one recent example of many, we are all aware of the tragic series of tornadoes that ripped through the nation's heartland this year, causing billions of dollars in damages, killing hundreds, and leaving thousands homeless.

A top priority for DHS is improving the communications capabilities of those who are often the first to arrive at the scene of a disaster site—the Nation's emergency responders. Public safety personnel must have access to reliable and instantaneous communications at all times to effectively coordinate response and recovery operations. The Department recognizes that establishing emergency communications is not solely a technology problem that can be solved with just the "right" equipment or the "right" communications system. All of the critical factors for a successful interoperability solution—governance, standard operating procedures, training and exereises, and integration of systems into daily operations *as well as* technology—must and are being addressed through the collective work of our programs.

Further, DHS believes that effective emergency communications requires continued partnering with the millions of emergency responders that are the first to arrive on the scene of an incident, as well as non-governmental organizations, the general public, and citizens of affected communities. We look forward to discussing our respective efforts and key accomplishments to make the nation more prepared in an all-hazards environment.

Emergency Communications Responsibilities
Within the National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) are two organizations that focus on different but converging areas of telecommunications in support of emergency operations: the Office of Emergency

67123.241

Communications (OEC) and the National Communications System (NCS). OEC and NCS are critical to shaping national policy and both work with other DHS components, federal departments and agencies, multiple levels of government, and the private sector to improve communications capabilities and achieve their mission requirements.

OEC was established as part of the congressional response to the communications challenges faced during the September 11, 2001, terrorist attacks and Hurricane Katrina in 2005. OEC coordinates policy and assists in the development and implementation of operable and interoperable emergency communications capabilities for emergency responders at all levels of government, including federal, state, local, tribal, and territorial. OEC also led the development of the first National Emergency Communications Plan (NECP).

The NCS, transferred from the Department of Defense to DHS in 2003, was created by executive order under President Kennedy to support the telecommunications functions of the Executive Office of the President and all federal departments and agencies for Continuity of Government, Enduring Constitutional Government, and Continuity of Operations. Presidents Reagan and George W. Bush each issued executive orders that evolved the responsibilities and structure of the NCS. Today, the NCS is an interagency system comprised of the telecommunications assets of 24 federal departments and agencies, each with significant operational, policy, regulatory, and enforcement responsibilities. The NCS coordinates telecommunications preparedness, response, and restoration activities across its 24 member agencies through the NCS Committee of Principals, which consists of senior government officials from each of the 24 member agencies, ensuring a diverse representation across the NCS that includes the full range of federal telecommunications assets.

Office of Emergency Communications

The creation of OEC was an important step toward improving the communication capabilities of those who are often the first to arrive at the scene of an incident—the nation's emergency responders. Inadequate emergency communications have been a critical gap in our nation's preparedness, and previous efforts to address this issue were hampered by the lack of a strong partnership between the Federal government and the public safety community. In addition, the nation lacked an overarching strategy to guide emergency communications planning and build capabilities at all levels of government.

In the last four years, OEC has worked to fill many of these and other gaps, and we are seeing progress in several key areas that enable emergency responders to interoperate in an all-hazards environment. As part of its mission, OEC led a comprehensive nationwide planning effort with more than 150 stakeholders from the emergency response community to develop the NECP. This included significant feedback and coordination with the SAFECOM Executive Committee, the SAFECOM Emergency Response Council, and the National Public Safety Telecommunications Council. These stakeholder groups represent the interests of millions of emergency responders, as well as the state and local governments that public safety communications serves. Involving these groups from the beginning ensured that the plan took stakeholders' input into account and would be widely accepted in the public safety community.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00616 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.242

In the almost three years since it was released, the NECP has been instrumental in defining communication priorities for public safety personnel at all levels of government. OEC has been driving implementation of the NECP in coordination with its federal, state, and local partners, and we are seeing measurable improvements with building capabilities and closing gaps identified in the plan for governance, training, operating procedures, and others, including:

- **Enhanced Statewide Coordination:** The creation of Statewide Communication Interoperability Plans (SCIPs), Statewide Interoperability Coordinators (SWICs) and Statewide Interoperability Governing Bodies (SIGBs) has improved coordination of emergency communications activities and investments throughout all 56 states and territories. Through the SCIP development and updating process, the SWICs, in collaboration with their SIGBs, have been effective in helping states define their communications needs and future investments and ensuring that federal funding is directed where it is needed most. In addition, OEC has conducted nearly 150 workshops over the past three years to assist states as they implement and update their SCIPs.

- **Common Plans, Protocols, and Procedures:** The use of standardized plans and procedures is driving improved command, control, and communications among emergency responder agencies in the field. To facilitate this, OEC and FEMA have worked with more than 140 jurisdictions, including Urban Area Security Initiative (UASI) regions, to develop Tactical Interoperable Communications Plans that document formalized interoperability governance groups, standardized policies and procedures, and emergency communications equipment inventories. States continue to develop these communications plans to cover additional regions.

- **Targeted Technical Assistance:** OEC has implemented a technical assistance strategy to ensure that all states and territories can request and receive its targeted, on-site emergency communications assistance, while also focusing support on the states and urban areas most in need. These offerings are tailored to support the priorities in each state's or territory's SCIP and the objectives of the NECP. Since 2008, the 56 states and territories have combined to request more than 750 individual technical assistance services from OEC for support with the development of governance structures, tactical and strategic planning, and a variety of engineering services.

- **Increased Training Opportunities:** OEC has developed Communications Unit Leader (COML) and Communications Technician (COMT) courses to improve emergency responders' proficiency with communications equipment and to assist them with coordinating roles and responsibilities during an incident or event. The COML program has been embraced by emergency responders nationwide, and OEC has trained more than 3,500 responders, technicians, and planners to lead communications at incidents across the nation, including local floods, blizzards, and wildfires. Trained COMLs have also contributed to recovery efforts throughout the United States, including the recent outbreak of tornados and massive flooding in the Midwest and Southeast.

- **Enhanced Border Communications and Coordination:** OEC has been actively working with our international partners at the Northern and Southern borders to improve

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00617 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.243

cross-border interoperable communications planning, policy development, and operations communications. DHS recently awarded $25 million in grant funding to states and local communities under the Border Interoperability Demonstration Project—a one-time competitive grant program focused on developing innovative solutions to strengthen interoperable emergency communications along the U.S. borders with our partners in Canada and Mexico.

- **Improved Governance and Coordination:** OEC is working with federal, regional, state, and local agencies to increase coordination, information sharing, and oversight of interoperability through formal governance structures and partnerships. For example:

    - SIGBs have been created in every state and territory and include representatives from all levels of government to coordinate and support statewide interoperability. The State of Indiana, for example, has implemented an effective governance process for emergency communications through the Statewide Interoperability Executive Committee, which also serves as an advisory group to the State's Integrated Public Safety Commission. Many states have also implemented Regional Interoperability Committees to provide insight into the statewide strategy from an operational perspective.

    - OEC continues to receive insightful feedback and input from responders, associations, and emergency communications professionals through the SAFECOM Executive Committee, SAFECOM Emergency Response Council, and the newly chartered National Council of Statewide Interoperability Coordinators.

    - OEC recently instituted a Regional Coordination Program to strengthen collaboration and knowledge sharing with our stakeholders. OEC has established a Regional Coordinator in each of the 10 FEMA Regions, and they regularly participate in the SIGBS, the UASI interoperability meetings and their respective FEMA Regional Emergency Communications Coordination Working Groups.

    - The Emergency Communications Preparedness Center (ECPC) provides an inter-departmental mechanism to coordinate common solutions, streamline development of policy and plans, and jointly engage state, local, and tribal partners. The ECPC has achieved early successes through defining a strategic agenda that reflects shared member priorities and establishes issue-specific focus groups to drive immediate action. Key accomplishments include: (1) coordinated inputs on national policy, such as federal agency comments on the Federal Communications Commission's (FCC) National Broadband Plan; (2) developed and published recommendations for common federal grant guidance to synchronize emergency communications spending across more than 40 grant programs; (3) initiated efforts to drive capability and resource sharing through mapping and analyzing existing federal communications resources; and (4) implemented a clearinghouse capability and data repository to yield improved information sharing and coordination.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00618 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.244

- To complement inter-governmental activities, OEC facilitates the Department's One DHS Emergency Communications Committee. This committee, comprising senior executives from the Office of the Secretary and the Components, provides a vital mechanism for maximizing the efficiency and effectiveness of the Department's emergency communications investments and activities. The One DHS Committee reached its most significant milestone recently with the creation of the first-ever unified One DHS Emergency Communications Strategy. The Strategy establishes a common vision "to ensure access to and exchange of mission-critical information across the Homeland Security Enterprise anywhere, anytime, through unified capabilities." The Strategy also sets goals for coordinating and improving emergency communications architecture, investment, governance, and operations.

Further, OEC and FEMA have partnered on the Interoperable Emergency Communications Grant Program (IECGP), which has been a primary vehicle for implementing the Department's interoperability goals. It has been instrumental in advancing the state of interoperable emergency communications throughout the nation, especially through its emphasis on:

- Establishing governance bodies that conduct strategic planning and prioritize investments;
- Supporting SWICs who ensure federally funded projects align to strategic plans; and
- Funding the implementation of NECP Goals, allowing DHS to measure progress in emergency communications capabilities nationwide.

OEC has also partnered with the DHS Science and Technology (S&T) Directorate to promote the effective use of Federal grant funding through the development of the SAFECOM Grant Guidance.

By focusing on these core capabilities—planning, governance, training, interagency coordination, and technology support—emergency response agencies are becoming more equipped to establish and maintain interoperable communications during response and recovery activities. One such example of how this is translating into "real world" success can be seen in Louisiana, where recovery operations have benefitted from years of governance planning, relationship building, and communications training. Using lessons learned and improvement efforts associated with Hurricane Katrina, Louisiana statewide officials are invested in improving interoperable and operable communications throughout the State, including the deployment of a robust statewide communication system for public safety use.

The State's standards-based system—called the Louisiana Wireless Information Network—has effectively supported interoperable communications performance during evacuation efforts for Hurricane Gustav and, more recently, the response to the BP oil spill. Interagency coordination was tested from the moment that the explosion occurred last April, and local responders were able to successfully communicate with each other and with the United States Coast Guard.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00619 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.245

Louisiana also coordinated with surrounding states to create talk groups designated for the spill and effectively used trained COMLs to initiate the process of action planning and lead major communications efforts throughout operations, including connecting multiple systems from surrounding states. Of course our hope is that another large incident in the Gulf will never happen, but if it does, Federal, state, and local agencies have demonstrated that they are more prepared and coordinated than ever before.

NECP Goal Assessments

Implementation of the NECP has been a key driver behind much of our progress in improving interoperability. More than 85 percent of the NECP milestones have been achieved to date, and progress is evident in all of the NECP priority areas, such as governance, training, and coordination. Nevertheless, considerable work still remains to achieve the long-term vision of the NECP, in which emergency responders can communicate as needed, on demand, as authorized, at all levels of government and across all disciplines.

To move the nation even closer to that vision, OEC is engaged in a comprehensive, nationwide assessment of emergency communications capabilities as it implements the NECP Goals. When complete, this assessment will provide a detailed view of capabilities at the county or county-equivalent level in all 56 states and territories. This detailed look at emergency communications—the first of its kind—will generate valuable data for both DHS and the states to use to more effectively and efficiently focus future resources and improvement activities.

OEC recently completed the measurement of Goal 1 of the NECP, which focused on emergency communications capabilities in the nation's largest cities. To measure NECP Goal 1, OEC worked with the UASI regions to assess their ability to demonstrate response-level emergency communications during a real-world event in each region. This approach enabled OEC to evaluate their use of emergency communications in real-world settings and in an economically efficient manner.

The results have been encouraging. Based on the capabilities documented at each Goal 1 event, all 60 urban areas were able to demonstrate the ability to establish response-level emergency communications in accordance with NECP Goal 1. This illustrated how the significant organizational and technical investments made by the UASIs have improved their emergency communications capabilities in recent years. In fact, OEC saw measurable improvements over key gaps identified in the previous DHS assessment of these urban areas in 2007, the *Tactical Interoperable Communications Scorecards* report. Some of these areas of progress were the result of DHS programs and funding, including the following:

- **Grants:** The NECP Goal 1 results showed an increase in the number of UASI regions using Project 25 (P25) digital radio standards-based systems, which are designed to allow interoperability regardless of equipment vendor. The implementation of P25 systems has been a provision in DHS grant guidance for several years, including the SAFECOM grant guidance and the Public Safety Interoperable Communications Grant Program.

- **Training and Technical Assistance:** As previously discussed, OEC offers a COML training program that has trained more than 3,500 responders, technicians, and planners

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00620 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.246

to lead communications at incidents across the nation. This program began in part as a response to gaps identified in the 2007 DHS Tactical Interoperable Communications Plans Tactical Interoperable Communications Plan (TICP) Scorecard assessment, specifically the lack of trained COMLs. During the NECP Goal 1 events, OEC found that a large majority of the UASI regions had assigned DHS-trained COMLs to handle planning and implementing multi-system communications for the event.

- **Exercises:** Almost all UASI regions reported that agencies within their regions are now holding communication-specific exercises, and approximately half of them reported that the agencies are holding these exercises on a regular basis. This represents significant progress over similar findings from the DHS TICP report in 2007, which concluded that "almost no [UASI] region had completed a communications-focused exercise before the TICP validation exercise."

OEC is currently in the process of implementing Goal 2 measurement, which calls for an assessment of emergency communications performance and capabilities at the county level (or county-equivalent level, such as parishes in Louisiana). This is a large undertaking, as there are more than 3,000 counties in the United States. OEC is working closely with the states and territories to complete this assessment by the end of this year and will be following up with them on how to use the results to update their SCIPs and more effectively utilize resources. From a DHS perspective, we believe the NECP Goals assessment will generate much needed capability data to more strategically direct federal and state emergency communications resources—including grant funds and technical assistance support—to where they are needed most.

Public Safety Broadband Network

Over the last decade, our Nation has made critical strides in strengthening overall security and national preparedness. The public safety community also has made significant progress improving emergency communications capabilities through enhanced coordination, planning, training, and equipment.

However, we have been limited by wireless technologies that were introduced decades ago. To fully achieve the vision of the 9/11 Commission, emergency responders must have an advanced, nationwide, inherently interoperable, public safety communications network. Recent developments in high-speed, wireless communications technology represent a new opportunity for emergency responders to have significantly greater operability, interoperability, and capability.

These broadband advancements can provide emergency responders with access to information that will improve their ability to safely and efficiently manage their daily activities and respond to all levels of emergency situations. For example, as President Obama stated in his State of the Union Address, these advancements can enable a firefighter to use a handheld device to download the design of a building before arriving at the scene of an emergency. These types of capabilities have the potential to save countless lives. That is why the Administration has been coordinating with the public safety community, the private sector, and Congress to promote initiatives for the deployment and development of a Nationwide Public Safety Broadband Network.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00621 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.247

Earlier this year, President Obama outlined his commitment to the development and deployment of such a network for public safety, a key recommendation from the *9/11 Commission Report*. The Administration's program in support of such a network is a component of its Wireless Innovation and Infrastructure Initiative, which was outlined in its Fiscal Year 2012 Budget. The public safety elements of the Initiative include an accounting for the foregone auction revenues resulting from reallocation of the D Block for use in the public safety broadband network; $7 billion in direct financial support for network deployment; $500 million for development and testing of broadband public safety requirements, standards and software applications (to be administered through the National Institute of Standards and Technology); and $5 billion for support to rural broadband services, including public safety services.

The Administration is fully committed to working with Congress to ensure the passage of legislation that meets the critical national need of establishing a public safety broadband network. We appreciate the bipartisan Congressional leadership on this issue that crosses committees of jurisdiction, including Chairman Lieberman, Chairman Rockefeller, and Senator McCain. We are confident that through continued cooperation with Congress, we can deliver a network that meets the needs of America's first responders whom all Americans rely upon.

OEC has been extremely active in support of the President's Wireless Innovation and Infrastructure Initiative and helping prepare the nation's responders for the deployment of broadband. OEC has worked closely with its federal partners at the Departments of Commerce and Justice to help set the broad policy framework for the planned network, and has coordinated with its state and local partners to ensure the public safety community's requirements are fully represented in network broadband planning and implementation efforts. More specific examples include the following OEC broadband-focused programs and activities:

- **Policy and Planning**: OEC is preparing an addendum to the NECP for release later this year that will identify key broadband challenges and recommend near-term actions to foster the integration of broadband technologies and data capabilities. This addendum also will propose further measures to support current interoperability efforts and to maintain existing Land Mobile Radio communications capabilities until broadband technologies can support mission-critical communications for first responders.

- **Outreach and Coordination:** OEC is working with all of its stakeholder groups—including the SAFECOM Executive Committee and Emergency Response Council, National Council of Statewide Interoperability Coordinators, ECPC, and the One DHS Committee on Emergency Communications—to ensure the views and requirements of the public safety community are fully represented in broadband planning and implementation efforts.

    - OEC supports outreach efforts related to the development and deployment of a nationwide public safety broadband network to include operational requirements, funding, standards, spectrum requirements, and governance. This includes support for an Innovation Roundtable with representatives from government, associations, public safety, and industry. OEC is also supporting a committee of

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00622 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.248

jurisdictions that received FCC waivers for early deployment of 700 MHz broadband systems as they begin their efforts to build networks. Through these efforts, OEC is continuing to emphasize the need for planning and good governance, since these elements of emergency communications have yielded progress to date.

- OEC continues to coordinate with the emergency response community, preparing wireless broadband guidance documents for SWICs, urban area and regional interoperability coordinators, public officials and executives, and emergency responders to support current NECP initiatives on interoperability planning. OEC also continues to provide emergency response stakeholders up-to-date and comprehensive information about wireless broadband in the emergency response environment. In addition, OEC is working with states and jurisdictions to incorporate broadband initiatives into the SCIPs.

- To increase coordination of federal efforts for broadband implementation, the ECPC is working to identify federal broadband requirements, preparing a consolidated view of emergency communications assets, addressing associated legal and regulatory barriers, developing departmental positions on pending broadband regulatory matters and rulemakings, and establishing standardized grant guidance and processes. The ECPC has identified the development of broadband standards and research and development as one of its strategic priorities for the coming year.

- Concurrently, the One DHS for Emergency Communications Committee is providing consolidated departmental input into federal interagency efforts, as well as developing strategies for broadband technology migration (i.e., transition from current land mobile radio technology).

- **Grants:** OEC's current SAFECOM grant guidance, which includes input from state, local, territorial, and tribal responders, contains a number of key provisions pertaining to broadband deployment. Further, the *ECPC Recommendations for Federal Agencies: Financial Assistance for Emergency Communications*, a document for federal emergency communications grant programs, will include updated guidance concerning the deployment of the Nationwide Public Safety Broadband Network.

- **Technical Assistance:** OEC has developed a wireless broadband technical assistance offering for 2011 to assist state, local, territorial, tribal and regional users develop and improve their use of broadband technology in line with the vision of a nationally interoperable network. The offering, which can be tailored for each jurisdiction, will provide informational briefings, governance models and standard operating procedures, project planning, and engineering support.

In addition, NCS provides technical advice to OEC regarding communications standards to ensure the proposed public safety network is interoperable with the commercial communications

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00623 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.249

networks. NCS also ensures that the priority functions for national security emergency preparedness function seamlessly as they operate between the networks.

National Communications System
Since its inception, NCS has developed programs and services to address the unique communications challenges associated with communications divestiture, deregulation, natural disasters, and terrorist attacks on our nation.

As the co-lead for Emergency Support Function #2 (ESF-2) – Communications, under the National Response Framework, NCS coordinates government and industry during planning for and response to disasters and major outages. The operational arm for communications activities is the 24/7 National Coordinating Center for Telecommunications (NCC), which coordinates emergency response operations supporting the National Response Framework. The NCC is, and has been, a consistent coordinating mechanism for managing efficient communications restoration and recovery activity for more than 25 years. The NCC also coordinates the communications assets of the NCS members to provide communications assistance during disasters (manmade or natural). During a response, the NCC also provides requirements priorities to industry partners.

NCS also manages government industry partnerships to assist decision-makers in understanding the risks to the Communications Sector. Under Homeland Security Presidential Directive 7, NCS is the sector-specific agency for the Communications Sector and coordinates government and industry partners under the Critical Infrastructure Protection Advisory Committee Act to reduce communications sector risk. NCS also manages the President's National Security Telecommunications Advisory Committee (NSTAC), which comprises 27 Chief Executive Officer-level members from communications, information technology, and defense corporations. Most recently, the NSTAC examined four scenarios designed to stress future 2015-level networks, and provided the President with recommendations for technology enhancements and government investments that would provide the best network resilience and recovery.

NCS capabilities include the following:

- **Operational Activities:** NCS develops and maintains NS/EP communications priority services programs, such as the Government Emergency Telecommunication System (GETS) and Wireless Priority Services (WPS), which provide users with priority on commercial networks. The GETS program is a White House-directed emergency telecommunications service managed by NCS. GETS supports over 274,000 federal, state, local, and tribal government, industry, and non-governmental organization personnel in performing their NS/EP communications missions by providing a robust mechanism to complete calls during network congestion from anywhere in the United States. Specifically, GETS provides 90 percent or more call completion rates when network call volume is up to eight times greater than normal capacity. For example, approximately 10,000 GETS calls were made with a 95 percent success rate during the 9/11 attacks, and 1,231 GETS calls were made with a 90 percent or more success rate during the 2003 Blackout.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00624 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.250

WPS is a nationwide program that provides priority NS/EP telecommunications via selected commercial wireless carriers. This program enhances the ability of 108,000 NS/EP subscribers to complete calls through a degraded public switched telephone network during a crisis or emergency situation. WPS calls receive the next available radio channel during times of wireless congestion and helps to ensure that key NS/EP personnel can complete critical calls by providing priority access for key leaders and supporting first responders. WPS service provides authorized cellular users with the ability to have priority within the public switched telephone network as well as access to priority channels.

The Telecommunications Service Priority (TSP) Program authorizes and provides priority treatment of NS/EP telecommunications services. The TSP Program provides service providers with an FCC mandate for prioritizing service requests by identifying those services critical to NS/EP. For example, a telecommunications service with a TSP assignment will receive priority by the service vendor before a non-TSP service. The TSP Program has two components: restoration and provisioning. A restoration priority applies to telecommunications services to ensure restoration before any other services. A provisioning priority is obtained to facilitate priority installation of new telecommunications services in response to an emergency. In addition to daily operations, TSP Program Office personnel are notified of presidentially declared disasters; activation of the National Response Framework, ESF-2; and Continuity of Operations and Continuity of Government (COOP/COG) plans. TSP Program Office personnel are on call 24/7. TSP can save days to weeks on the time required to return wireline voice/data services, and there are more than 200,000 active TSP circuit assignments in support of NS/EP communications.

NCS continues to migrate GETS and WPS services to work across evolving networks. NCS works with industry to enhance and assure these priority programs are compatible with Next Generation Network (NGN) technology.

The Modeling, Analysis, and Technology Assessments team provides expertise in modeling and analyzing current and future protocols, algorithms, network designs, and capabilities that will impact priority service communications in legacy and NGNs. The modeling team also maintains a suite of specialized infrastructure analysis tools to provide critical infrastructure risk assessments for the communications sector in the event of a man-made or natural disaster. The assessments consist of the following:

- Providing technical analysis of current and next generation communications systems, new technologies, physical and logical architectures, and products related to communications network infrastructures.

- Determining new and emerging communications technologies under various congestion and failure conditions to identify vulnerabilities and predict performance of existing and next generation networks.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00625 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.251

- Developing products to be used for COOP/COG functions during disaster response related to federal, state, local and tribal governments.

- **Standards Activities:** The NCS Standards Team is an active leader and contributor to various national and international standards developing organizations, ensuring industry-wide adoption of non-proprietary solutions for NS/EP preparedness telecommunications requirements.

  The Team provides leadership and representation in standards bodies to recommend standards that, when implemented in Internet Protocol-based networks, will provide capabilities to ensure national, state, and local leaderships' ability to communicate during times of crisis.

  The Third Generation Partnership Project, known as 3GPP, is focused on the technical aspects associated with provisioning priority services in Long Term Evolution networks and is being pursued under the enhanced Multimedia Priority Service project. In cooperation with the Alliance for Telecommunications Industry Solutions (ATIS), NCS is developing an End-to-End Next Generation Network GETS Service Call Flow Standard that specifies end-to-end call flows. ATIS is also developing the baseline text for an Emergency Telecommunications Service wireline access requirements standard. This standard details the network element requirements for wireline access in support of Digital Subscriber Line, Cable, Fiber, and Metro Ethernet.

- **National Response Planning:** NCS is working with federal, regional, state, and local agencies to increase communications coordination, information sharing, and oversight of emergency preparedness activities to improve response to man-made and natural disasters. NCS works with these entities to ensure a coordinated response through formal governance structures and partnerships.

International Interoperability
DHS is working with its international partners to enhance interoperable communications to bolster information sharing and coordination among law enforcement personnel around the world.

For example, the United States and Mexico are establishing a new cross-border communications network, which will improve incident response and coordination among participating federal, state, local, and tribal law enforcement and public safety personnel along the border. Installation is scheduled to begin this summer. DHS and Public Safety Canada also work together to enhance cross-border interoperable communications planning, policy development and operations through the annual Canada-U.S. Cross-Border Interoperable Communications Workshops.

Conclusion
The Department appreciates the Committee's support for our interoperable emergency communications activities. Thank you again for this opportunity to testify. I would be pleased to answer your questions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00626 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.252

Testimony to the United States Senate Committee on Homeland Security and Governmental Affairs

July 27, 2011

Ten Years After 9/11: Improving Emergency Communications

Michael D. Varney
Statewide Interoperability Coordinator
Connecticut Department of Emergency Services and Public Protection

67123.253

Introduction:

Chairman Lieberman, Ranking Member Collins, and distinguished members of the Committee, I would like to thank you for allowing me the opportunity to provide testimony on this important topic.

I am Michael Varney, the Statewide Interoperability Coordinator for the State of Connecticut. In addition, I serve as the Vice Chairman of the National Council of Statewide Interoperability Coordinators. During my testimony I will speak as the Connecticut Statewide Interoperability Coordinator as well and representing the National Council of Statewide Interoperability Coordinators (NCSWIC). I have worked in the emergency services, information technology and communication fields for over 24 years and have served in the capacity as the Connecticut Statewide Interoperability Coordinator for over six years.

Being a local first responder and serving in the capacity as a fire chief and hazardous materials team commander, I can truly appreciate the efforts put towards solving the nationwide interoperability problems, having seen their positive impact directly in the field.

Close to ten years ago since the attacks of September 11th, 2001 a priority for States has been improving emergency responder communications capabilities. Public safety responders need the ability to have the most accurate, reliable information and be able to communicate directly and instantaneously with their assisting and supporting responders.

We understand that solving this interoperable communications problem is more than a technology problem alone. This problem requires significant efforts in governance, standard operating procedures, training and exercises, and the use of these systems in daily operations.

Public safety communications interoperability takes significant coordination to solve and is being addressed by the creation and use of Statewide Interoperability Coordinators or SWICs.

Through the Department of Homeland Security's Office of Emergency Communications the role of the SWICs and their position has been defined and substantially increased. In each state and territory there is a designated SWIC responsible for a variety of critical planning and coordinating functions, all of which were not coordinated through a specific designated office prior to 2001.

For States to improve communications interoperability, collaboration and participation from relevant emergency response stakeholders is essential. In Connecticut, our Statewide Public Safety Interoperable Communications Committee has representatives from each of the five emergency management and homeland security planning regions within our state, law enforcement, emergency medical services, fire departments and key state and federal response and planning agencies. The abilities and relationships that leveraged by this group have been very successful in our efforts to improve public safety communications interoperability within Connecticut and with our surrounding states.

67123.254

As the central coordination point for their State's interoperability effort, the SWIC plays a critical role. SWICs are responsible for the implementation of the Statewide Communication Interoperability Plan (SCIP) through collaboration with the emergency response community. These individuals dedicate considerable time towards educating the public safety community on their SCIP and enhancing their statewide governance structures. The SWIC also plays a crucial role in the facilitation of governance, training and exercise, and policy efforts to further interoperability across all disciplines of emergency responders. The SWIC's implementation efforts are guided by the initiatives outlined in the National Emergency Communications Plan (NECP) and Statewide Communication Interoperability Plans (SCIP).

Efforts that are currently underway by the nation's SWICs include; the coordination and outreach regarding the 2013 narrow banding mandate, the development of intrastate regional governance, development of standard operation procedures and memorandums of understanding, the development of Interoperable Field Operations Guides at the state, urban area and regional level, for use, wireless broadband planning, and each States Communications Unit Leader Training and Certification programs.

Each of the designated Urban Area Security Initiative (UASI) site developed a TIC Plan using a national framework put in place. Connecticut used this framework to continue to create TIC Plans for all of the additional emergency management and homeland security planning regions in our state. This effort was possible because of the Interoperable Emergency Communication Grant Program (IECGP) funding. Since the TICPs have been developed they have been used in the field by local practitioners to successfully plan for and respond to events and emergencies that involve multiple disciplines and jurisdictions. The plans helped successfully provide for communications to several large scale law enforcement and hazardous material incidents, responded to by multiple agencies. In early June when tornados struck southern Massachusetts, the Connecticut fire service was requested and responded with significant assets which were coordinated quickly and efficiently between the two states due the prior planning and exercises made possible through the IECGP funded TIC Plan process.

Goal 2 of the National Emergency Communications Plan (NECP) states that by 2011, 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies. This is currently being measured and data collected through the SWICs using assistance and tools developed though DHS Office of Emergency Communications (OEC). The SWICs are implementing the Goal 2 measurement process to be completed later this year, which calls for an assessment of the over 3000 counties in the United States of emergency communications performance and capabilities. This important assessment information will be used to update the SCIPs and prioritize the use of grant funds and assistance from coordinated by the SWICs.

The SWICs serve as members of the National Council of Statewide Interoperability Coordinators (NCSWIC), which was established in 2010 to assist State and Territory interoperability coordinators with promoting the critical importance of interoperable communications and the sharing of best practices. As a member of the NCSWIC, the SWIC

67123.255

plays a key role in preparing public safety responders through the development of bottom-up governance structures, standard operating procedures, strategic development and implementation of voice and data technologies, training, exercising, outreach and technology usage. The NCSWIC members enhance the response capabilities of public safety responders through close coordination and collaboration with all levels of government.

As a SWIC I cannot say enough about the excellent support and engagement by the DHS Office of Emergency Communications. Their technical support and coordination activities have proven invaluable to our efforts in Connecticut. Connecticut has developed and updated our Statewide Communication Interoperability Plan, created intrastate governance, provided technical training, and data collection activities with the technical assistance from OEC. OEC has through this process and other outreach activities through SAFECOM and the NCSWIC listened to our concerns and priorities and adapted their programs and deliveries to make them as relevant as possible. Truly providing stakeholder driven products and services.

As I mentioned earlier the IECGP funds such as those used to create TICPs in Connecticut have been critical to the SWICs. IECGP funds have been used by the SWICs for planning, training, narrowbanding and public safety broadband activities, and to establish governance initiatives. The IECGP provides funding for the SWICs to ensure that federally funded projects align to strategic plans, and to implement and report on the NECP Goals, allowing DHS to measure progress in emergency communications capabilities nationwide.

In a survey of SWICs conducted in June we found that over one third of the SWIC positions were funded in whole or part by this grant program. The elimination of the funding of this program and reduction of related homeland security grant programs will have a direct impact on the sustainment of the many programs put in place to increase interoperable communications. We appreciate your committee's ongoing support and commitment to the many Homeland Security Grant Programs, specifically the Interoperable Emergency Communications Grant Program.

In Connecticut as the SWIC, I also help coordinate communications support to emergency responders in a disaster environment. As part of this effort, we are an active member of the FEMA, Region 1 Regional Emergency Communications Coordination Working Group. This group comprised of state, local and federal organizations provides us a forum meet with our peers from New England to network and develop specific plans for the deployment of assets for on scene communications support in the event of a disaster. It also is a forum to let us assess and address the sustainability and interoperability of emergency communications systems at all government levels.

We are aware of the commitment to the development and deployment of a nationwide, interoperable wireless network for public safety the administration has put forward in the President's Wireless Innovation and Infrastructure Initiative and helping prepare the nation's responders for the deployment of broadband. Many of our issues are captured within the Rockefeller-Hutchinson bill (S 911), and we are very appreciative of Senators Lieberman and McCain's leadership and the Homeland Security and Governmental Affairs Committee in their work to reallocate the 'D' Block for public safety use. This leadership will ensure successful completion of this very important milestone.

67123.256

While maintaining their traditional land mobile radio systems, our public safety agencies are increasingly using commercial broadband systems to support their missions. We have been relying on off the shelf broadband systems using laptop computers in vehicles and communication devices such as blackberries and smart phones for remote data communication.

Although the present commercial broadband devices have some functions that go beyond public safety communications devices, they lack the ruggedness, reliability, rapid calling and conferencing, and direct device-to-device connectivity of traditional public safety radio systems and equipment. In other words commercial networks do not provide the public safety control, mission criticality, capacity needed for their mission.

The statewide Interoperability Coordinators believe the creation and support of an interoperable wireless broadband network for public safety is critical for interoperability and to allow first responders to communicate and do their jobs as safely and efficiently as possible. We appreciate your ongoing support to make this nationwide network a reality. The NCSWIC is very appreciative of the initiatives supported by the homeland security and governmental affairs and commerce committee to create a nationwide public safety broadband wireless network.

These initiatives by reallocating 700 MHz D block spectrum to public safety, take advantage of the unique opportunity to dedicate sufficient contiguous spectrum to first responder communications by establish a funding source for construction and operation of the network and address key governance issues necessary to ensure nationwide interoperability. The SWICs in each state working with their established governance groups are uniquely positioned to address wireless broadband planning due to the existing governance and relationships of the key practitioners in the field.

Right now my son and daughter have more capability than my firefighters do responding to emergencies everyday. This is a unique time to solve this problem and create a nationwide public safety wireless broadband network.

We look forward to working with you and your senate colleagues to pass this law to meet public safety's needs for interoperable communications, a key recommendation from the 9/11 Commission Report.

In conclusion I again would like to thank the ongoing tremendous support and activity by your committee to increase interoperable communications throughout the United States. The federal investment to support interoperable communications programs over the past few years will continue to show its value in saving lives and protecting property while our nation's first responders work together to respond to emergencies and disasters in our homeland. Thank you again for this opportunity to testify. I would be pleased to answer your questions.

67123.257

Testimony

Senate Homeland Security and Governmental Affairs Committee

Ten Years After 9/11: Improving Emergency Communications

July 27, 2011

Senator Lieberman, Senator Collins, Members of the Homeland Security and Governmental Affairs Committee thank you for the opportunity to come before you this morning.

My name is Robert McAleer and I am the Director of the Maine Emergency Management Agency.

I would like to address the issue of communications interoperability as it relates to the State of Maine and in particular some the accomplishments we have achieved since 2001, our work that is currently in progress and existing gaps that need to be addressed.

By New England standards, Maine is a large state, roughly equivalent to the rest of the New England States combined. It is a mostly rural state with vast areas of very limited population and some very rugged terrain. Maine is also not a wealthy state. These factors have made improving interoperability a challenge.

Maine, however, has been fortunate to receive a significant amount of Federal funding, for which we are very grateful, to support our efforts. We estimate that approximately $9.5M or about 25% of our Homeland Security, Public Safety Interoperable Communications, and Interoperable Emergency Communications Grants funds have been dedicated to improving communications just since 2007. We have used that funding to leverage whatever local funding municipalities have generated to make notable improvements.

67123.258

One advantage that we have had throughout this process is that the vast majority of our first responders use VHF radios that broadcast and receive similar frequencies. We do have a couple of pockets, such as the Cities of Portland and South Portland, that operate on 800 MHz frequencies. These jurisdictions have taken steps to ensure they are able to communicate with neighboring communities.

Because of the overwhelming similarity in equipment state-wide, our challenge has been to replace old or worn out equipment and to acquire new equipment where there was none or to replace equipment that simply was inadequate to meet current needs.

In addition to acquiring a large number of modern radios for our first responders, we have completed numerous larger projects. Attachment (a) contains a detailed compilation of the projects since 2003. Among those projects are:

- $107K to upgrade communications systems throughout Sagadahoc County and complete their narrowband transition.
- $198K to upgrade the communications infrastructure for the Hancock County Sheriff's Office
- $500K for the bulk purchase of narrowband compliant fire pagers
- $346K to support a county-wide microwave communications project in Cumberland County
- The State acquired (4) large mobile command vehicles that have state of the art radio, cell phone, internet and satellite capabilities for use in incident coordination. In multiple instances, these vehicles have served as dispatch centers when fixed facilities were out of service. We have also provided support for communications vehicles in over half of our counties.
- The State has established radio caches at crossing sites along the US/Canada Border for use by first responders moving across the border to ensure adequate interoperable equipment is available.
- Each County now has portable repeater antennas that can be deployed to remote areas where coverage may be minimal or to boost signals that might be otherwise blocked.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00633 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.259

- Our largest and one of the most rural counties has a 100 foot tall vehicle mounted tower that can be deployed and operational within 20 minutes.
- We have been able to move our EOC from a facility that was generally inadequate to a new facility and provide the new EOC with equipment that meets virtually all of our communications needs.
- Our court system and law enforcement agencies now have access to a data broker system that enables almost instant access to the various types of critical information, such as protection orders.
- The majority of our law enforcement and even some fire departments now have Mobile Display Terminals in their vehicles which in many cases provide a better communications capability than standard radios.

We realize that interoperability is not just a matter of acquiring equipment. In many instances process and training also bring gains. Along those lines, we have established a Memorandum of Understanding (MOU) with the owners of six state-wide frequencies to allow incident commanders to request dedicated use of those frequencies to establish and coordinate communications at an incident. These so-called CONOPS Channels have been used during training events and actual incidents. The latest instance was this past weekend when multiple agencies were involved in traffic control at a large gathering.

We have also dedicated a significant amount of time to Communications Unit Leader Training. This training helps us ensure that there is sufficient expertise available at a large event to ensure that the correct agencies are speaking on the correct channels.

We have worked with our counties to ensure that they have up to date detailed county-wide communications plans to identify all of their communications assets, ensure that their procedures are adequate and to identify any gaps.

Our border with Canada has presented a unique challenge. To meet that challenge we have been conducting a series of cross-border communications working sessions with our local, state and federal partners on both sides of the border. The sessions are helping us

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00634 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.260

understand our differences and plan for how we can overcome those differences when needed. We will soon be publishing our Border Interoperability Plan to formalize our procedures and protocols.

In addition to these workshops, Maine, with the support of our Canadian partners, applied for and received a Border Interoperability Demonstration Pilot (BIDP) grant. Out of (21) applicants Nation-wide, Maine was (1) of only (7) awardees. We are using the almost $4M provided by this grant to significantly reduce communications gaps along the border and establish a single common frequency that will be available for use by first responders from both sides of the border.

Finally, the State of Maine is investing $50M of state funding to essentially rebuild and expand the infrastructure backbone of the State's communication system. When this project (MSCOMMNET) is completed, the State will have a series of 42 interconnected transmission towers that will replace infrastructure that has reached or passed its useful life expectancy, provide enhanced coverage and increase redundancy. Of note is that part of the tower build out is a joint effort between the State and our Customs and Border Patrol partners. We believe this may be the first such partnership in the Nation. Included with this project is the replacement of virtually all State-owned portable and mobile radios.

In general, Maine is in a relatively healthy position with regard to interoperability. Through the concerted efforts of many people and the judicious use of available resources, we have been able to accomplish a great deal. And we have witnessed those accomplishments coming in to play during real world events. There is, however, more work that needs to be done.

First and foremost in our view is the requirement to meet the FCC narrowbanding mandate. While the initial estimates of the cost to meet this requirement were staggering, we have dedicated a major portion of available federal funding to the requirement as well as a concerted effort to encourage local communities to recognize their own

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00635 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.261

responsibility to invest in the solution. Because we will be able to reallocate many of the state radios that are being replaced as part of MSCOMMNET, we believe that our first responders will be ready on January 1, 2013. We remain concerned about communities that are not meeting the National Incident Management System (NIMS) compliancy requirements because we cannot assist them with Federal funds.

We believe firmly, that during an emergency situation, if we do not have solid communications, then we will have no coordination. We will only have chaos. For that reason building a solid communications capability has been a priority for the State for a number of years. Further strengthening of that capability and sustaining what we now have will be priorities moving forward.

That concludes my testimony. I would be pleased to answer any questions you might have.

Thank you.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00636 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.262

Attachment (a)

FY2010 HSGP

- $107,000.00 was granted to Sagadahoc County. This investment completed a project to upgrade the communication system throughout the county to ensure that all first responders in the county have access to reliable radio communications as well as to fully implement CONOPS, complete the changeover to narrowband, and improve fire paging capabilities.

- $95,424.50 was granted to Waldo County. This investment leveraged the EOC Grant which Waldo County received to complete the communications infrastructure portion of the EOC to guarantee access to interoperable communications throughout Waldo County. Waldo County purchased an antenna, and multiple radios with these funds.

FY2009 HSGP

- $81,565.00 was granted to Aroostook County. This investment purchased a mobile radio tower that is used to ensure radio communications can be established in areas where otherwise there would not be access to a reliable communications infrastructure.

- $72,355.00 was granted to Washington County. This investment completed a multi-year, multi-phase project to completely modernize the microwave and line-of-sight communications systems that support the first responder community in Washington County.

- $73,034.00 was granted to the Kennebec County Sheriff's Office. This investment assisted the Sherriff's Office to complete a modernization project for their communications system and ensure that identified communications gaps were closed. The grant funds purchased a UHL link system, repeaters, and antennas as well as other communications equipment.

- $75,864.00 was granted to Knox County. This investment leveraged local funds to improve communications infrastructure throughout Knox County. It purchased simulcast equipment, radios, and repeaters, among other items.

FY2008 HSGP

- $87,413.18 was granted to the Lincoln County Regional Communications Center (RCC). This investment leveraged local funds which were dedicated to a modernization project to upgrade aging communications infrastructure. The grant funds were used to upgrade the repeaters for police and fire as well as bring the RCC's base station radio into narrowband compliance.

- $198,916.47 was granted to the Hancock County Sheriff's department to improve the department's communication's infrastructure. The grant funds allowed the Sheriff's

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00637 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.263

Office to modernize their communications system and ensure adequate communications pathways were available for law enforcement personnel.

- $82,644.00 was granted to the University of Maine's Public Safety Department to upgrade their Computer-Aided Dispatch systems.

- $77,610.00 was granted to Washington County to support a phase of their ongoing communications infrastructure upgrades. These funds purchased mobile and portable radios which were issued to first responder agencies.

- $124,213.00 was granted to a regional coalition of first responder agencies in the Winthrop area. This regional application took into account the communications needs of multiple jurisdictions and first response disciplines. The grant funds purchased 166 mobile and portable radios, 2 repeaters and related communications equipment.

The FY2007 Public Safety Interoperable Communications (PSIC) grant has allowed Maine to complete multiple communications interoperability projects.

- A cache of radios strategically located at Ports of Entry between Maine and Canada was purchased using $73,700.00

- $95,035.00 was granted to Maine's Office of Information Technology to purchase a mobile tower that can be used to replace damaged communications towers.

- Maine supported the statewide communications system, MSCommNet, with a grant of $847,646.72. Leveraging state funds dedicated to MSCommNet with PSIC grant dollars has assisted in building a more robust and complete communications infrastructure that will benefit all levels of government in the State of Maine.

- $153,932.92 was granted to Aroostook County to assist in a county-wide communications upgrade. The grant funds purchased 125 mobile and portable radios, antennas, frequency planning and related equipment.

- $72,917.25 was awarded to Cumberland County to purchase 55 portable radios for first responders.

- $346,310.00 was awarded to the Cumberland County RCC to support a county-wide microwave communications project to support the first responder community in Cumberland County.

- $75,540.67 was awarded to Franklin County to purchase mobile and portable radios as well as repeaters for first responders in Franklin County.

- $203,281.43 was awarded to the Knox County Sheriff's Office to support an upgrade to their communications system and computer-aided dispatch and records management systems.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00638 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.264

- $72,700.00 was awarded to the Knox County RCC to upgrade two of the microwave links crucial to their communications system.
- $301,677.55 was used for a bulk purchase of mobile and portable radios which were distributed state-wide to first responders.
- The Oxford County RCC received a grant of $286,923.00 to upgrade their microwave communication system backbone.
- $155,184.20 was granted to the Penobscot County RCC to upgrade their microwave communication system backbone.
- $262,044.31 was granted to the Penobscot County Sheriff's Office to improve their computer-aided dispatch system.
- Piscataquis County received a grant of $216,500.00 to upgrade their county-wide communications system.
- The city of Portland received a grant of $236,250.00 to upgrade the city's microwave communications system.
- $142,961.25 was granted to Sagadahoc County in the first phase of a county-wide communications upgrade project.
- $179,317.95 was granted to Somerset County to upgrade the county's communication system.
- Waldo County's project to replace the Aborn Mountain Communications tower was granted $242,030.60.
- $188,154.75 was granted to Washington County to support their multi-phase communications upgrade project.
- $235,305.00 was granted to York County to support an upgrade to their communications system; 93 mobile and portable radios were purchased as well as communications antennas and related equipment.
- $500,000.00 was awarded to Maine's Judicial Branch to support an upgrade to their data broker program.
- $500,000.00 was allocated state-wide for the purpose of purchasing narrowband compliant fire pagers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00639 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.265

FY2007 HSGP

- $93,587.10 was used by the State of Maine for a bulk purchase of 362 mobile and portable radios. These radios were distributed to local and county first responders.

FY2006 HSGP

- $260,285.50 was used by the State of Maine for a bulk purchase of 300 mobile and portable radios. These radios were distributed to local and county first responders.

- $314,747.00 was granted to Washington County. This was another phase of Washington County's microwave communications upgrade project.

FY2005 HSGP

- Waldo County received $80,000.00 to leverage local funds on their microwave communications upgrade.

- Somerset County's RCC received $150,000.00 toward their communications redundancy project.

- Maine spent $135,217.45 to equip 47 hospitals statewide with radio equipment.

- $426,943.99 was granted to Androscoggin and Franklin Counties for a joint Mobile Data Terminal project.

- $314,747.00 was granted to Washington County for another phase of their county-wide microwave communications upgrade project.

- Knox County law enforcement agencies received $200,000.00 toward microwave system upgrades, computer-aided dispatch and MDT systems upgrades.

- The towns of Verona, Bucksport, and Orland received a regional radios communications system upgrade grant of $59,650.00.

- Aroostook County received $186,478.36 for a communications tower, repeater link, mobile data terminals, and a radio dispatch console.

- $328,739.00 was granted to the City of Bangor for bi-directional radio amplifiers, dispatch consoles and other radio equipment.

- Maine's Office of Information Technology received $240,362.30 to upgrade the radio network dedicated to Maine's Department of Conservation.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00640 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.266

FY2004 HSGP

- $83,572.91 was granted to Washington County. This was the beginning of Washington County's microwave communications upgrade project.
- Lincoln County Sheriff's Office received a $102,951.00 as a grant to assist with an upgrade to their Mobile Data Terminals and Communication Tower infrastructure.

FY2003 HSGP

- $266,945.12 was granted to the Cumberland County Sheriff's Office to install a mobile data terminal system and purchase mobile and portable radios.
- $220,417.46 was granted to multiple law enforcement jurisdictions in Cumberland County to regionalize a mobile data terminal system.
- Somerset County Sheriff's Officer received a $64,550.00 grant to upgrade their computer-aided dispatch systems.
- $183,430.00 was granted to the cities of Raymond, Sebago, Casco, Harrison, and Naples to upgrade their communications systems including their computer-aid dispatch system.
- The City of Cape Elizabeth received $134,627.00 to upgrade their radio system.
- $477,191.00 was granted to the City of Portland to upgrade communication capabilities in the city.
- The City of Westbrook received a $98,305.00 grant for improvements to their computer-aid dispatch and records management systems.
- The Franklin County RCC received $73,118.00 to upgrade two radio communications consoles.
- The City of Augusta used $71,025.00 in grant funds for upgrades to their communications system.
- $113,757.11 was granted to Knox County to upgrade communication capabilities throughout the county.
- Lincoln County received a grant of $174,176.11 for communications systems upgrades.
- $117,588.40 was granted to Oxford County for the purchase of mobile and portable radios and repeaters.
- Sagadahoc County received a grant of $76,942.69 for the purchase of radios and pagers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00641 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.267

- $85,792.25 was awarded to Somerset County for the purchase of radios, pagers, repeaters, and consoles.
- Waldo County received $137,620.33 toward the purchase of radio repeaters.
- $93,474.76 was granted to Washington County's RCC for the purchase of radio console equipment.
- $185,774.56 was granted to York County for radios, pagers, repeaters, and radio antennas.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00642 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.268

Public Safety Alliance
Dedicated to First Responders...First

Hearing before the Senate Committee on Homeland Security and Governmental Affairs

Ten Years After 9/11: Improving Emergency Communications

July 27, 2011
Dirksen Senate Office Building

Testimony of Charles H. Ramsey
Police Commissioner, Philadelphia Police Department
President, Major Cities Chiefs Association
President, Police Executive Research Forum

67123.269

Good Morning Chairman Lieberman, Ranking Member Collins and all invited speakers and guests. Thank you for this opportunity to discuss a critical issue affecting all public safety and law enforcement organizations across our country, and our ability to serve the public. Having had 42 years in law enforcement, I have witnessed many important changes in emergency communications across police departments in three cities: first in Chicago for 30 years, then as Chief of the Metropolitan Police Department here in Washington, DC, for nine years, and now as Police Commissioner in Philadelphia for the past three and half years. I also have the privilege of serving as the President of the Major Cities Chiefs Association (MCCA) and the Police Executive Research Forum (PERF), both of which are members of the Public Safety Alliance (PSA).

The PSA is a coalition of the leading national public safety associations that represent every law enforcement, fire, EMS, emergency management agency and first responder organization in the country. I am here on behalf of first responders across this country to thank you, Mr. Chairman and Senator McCain for sponsoring bill S. 1040: The Broadband for First Responders Act of 2011.

We hope that you will also continue to work closely with Senator Rockefeller, Chairman, of the Senate Committee on Commerce, Science and Transportation, and sponsor of bill S.911: SPECTRUM Act, which was recently voted out of Committee for consideration by the Senate.

These bills fulfill an absolutely critical need. They allocate the D Block to public safety; provide the necessary funding to build out and expand the nationwide broadband network; and establish a governance structure in cooperation with state and local authorities.

Since September 11th, 2001, like many other jurisdictions around the nation, the Philadelphia region worked diligently to ensure adequate Local, State and Federal coordination for emergency communications. We established an "Interoperable Communications Committee" within our Southeast Pennsylvania Regional Task Force. Representatives from the five counties in the Philadelphia UASI, as well as seven additional regional counties from New Jersey, Delaware and Maryland comprise this task force. I'd like to thank Committee Member, Senator Tom Carper, for his assistance in strengthening homeland security in our region.

Let us be very clear in our mission: A terrorist attack or a major catastrophic event knows no municipal, state or federal boundary. Emergency preparedness spans across lines, and demands that law enforcement and public safety organizations across the country plan and coordinate their responses.

Mr. Chairman and Members of the committee, we have an extremely valuable opportunity in front of us to meet our needs in emergency communications. Seamless interoperability can

only be achieved through a dedicated public safety nationwide broadband network. The allocation of the D block for public safety organizations, with adequate capacity, control and funding, is the only proposal that will meet the challenges and demands that we confront. As President of MCCA and PERF, I am here to support this solution, which serves law enforcement and public safety organizations, and most importantly, helps to protect the American people in the best way possible.

Commercial networks are not designed to serve our public safety needs. Past experience with major national disasters have demonstrated that these networks are not interchangeable with dedicated public safety networks. There are fundamental differences in the architecture that go to the heart of public safety communications. The Public Safety Alliance will strongly oppose any legislation or resolution that supports auctioning the D block. Public safety becomes both less public and less safe if we auction any part of the D Block to the highest commercial bidder.

We need the upfront funding to jump-start the investment and build out of the network, and to attract and encourage commercial interest and competition. We will partner with the private sector to leverage and make maximum use of the existing infrastructure, while managing operations locally through a national governance structure.

This Committee, the House Homeland Security Committee, the House Energy and Commerce Committee, and the Senate Commerce, Science and Transportation Committee have all held numerous hearings over the past two years on the proposed public safety spectrum and the nationwide broadband network. Congress has asked many good questions, and hopefully you now have the information you need to make an informed recommendation.

Our first responders, who put their lives on the line every day, must have the resources that they need to do their jobs more efficiently and effectively, armed with real-time data, video and other critical information. We can only accomplish this goal if we have the latest in mobile broadband technology that is fully interoperable on a Local, State, and Federal level. The ability to share mission critical information nationwide to coordinate and plan our response to emergencies depends on having this capability.

I would like to thank all of the Members of the Committee for your continued time and commitment to finding a solution that will meet the communications needs of our first responders, and will best serve the American people. What Congress decides now will dictate the future of our emergency response capabilities. Ten years after 9/11, we urge you to make the decision that will finally establish a dedicated nationwide public safety broadband network.

I am happy to answer any questions that you may have now. Thank you for your time and consideration.

Post-Hearing Questions for the Record
Submitted to Gregory Schaffer
From Senator Joseph I. Lieberman

"Ten Years After 9/11: Improving Emergency Communications"
July 27, 2011

Question#:	1
Topic:	requirement
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Some first responder groups and the 9/11 Commission Chairmen (who, like I do, support allocating the D Block to public safety), have raised a concern about the lack of a requirement for interoperability across all band classes in the 700 MHz band. They have submitted that interoperability across the entire 700 MHz band would provide a number of benefits to public safety, such as providing interoperability for first responders on commercial networks while the D Block is being built out, providing redundancy for users of the D Block, and reducing equipment costs for first responders by creating a greater economy of scale for equipment that will be used in the 700 MHz band classes. What are the Department's views on this issue?

Response: Congress and the Federal Communications Commission could help support innovation in public safety equipment and produce economies of scale by requiring interoperability across all of the broadband portions of the 700 MHz band.

Question#:	2
Topic:	IWN
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In 2008, the Department chose to withdraw from the Integrated Wireless Network (IWN) program after issues arose concerning deployment and funding of the system. In the years since, the Department of Justice has continued the program in collaboration with the Department of Treasury and the U.S. Park Police, starting with the National Capital Region. I understand that certain agencies within the Department, including the U.S. Customs and Border Protection and the U.S. Coast Guard, may have an interest in participating in the program as it expands out to the rest of the nation. What process would an agency within the Department have to go through to take part in IWN, and how could they gain approval to do so?

Response: Several of the Department of Homeland Security's (DHS's) Components, including U.S. Customs and Border Protection and the U.S. Coast Guard, continue to participate in the Integrated Wireless Network (IWN) program, specifically in the Pacific Northwest Region and along the southwest border in San Diego. U.S. Immigration and Customs Enforcement has actively engaged in discussions with the Department of Justice (DOJ) Wireless Management Office to utilize the IWN in the National Capital Region. In addition, DHS components actively collaborate with the DOJ on current and emerging technologies that could augment current land mobile radio capabilities.

For an agency within DHS to join a deployed IWN system, the agency procures its own subscriber units (radios) and contributes to recurring operations and maintenance costs through a "fee for service" agreement established in a Memorandum of Understanding (MOU) with the DOJ. If an agency wanted to simply establish interoperability, with the IWN system, there would be no charge for this activity and such an MOU alone would suffice.

Post-Hearing Questions for the Record
Submitted to Gregory Schaffer
From Senator Carl Levin

"Ten Years After 9/11: Improving Emergency Communications"
July 27, 2011

Question#:	3
Topic:	projects
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: International Interoperability Demonstration Projects: Section 302 of the Improving America's Security Act of 2007 (Public Law 110-53) provides for the establishment of at least six interoperability demonstration projects (3 on the northern border, and 3 on the southern border) to facilitate interoperable communications across national borders expeditiously and help ensure that emergency responders can communicate with each other in the event of an emergency. On May 2, 2011, DHS announced funding for seven interoperability demonstration projects, the largest of which, a $4 million grant, went to Michigan State Police to strengthen their ability to communicate via radio with Canadian police [and other public safety officials??] in the event of an emergency.

What does the Department of Homeland Security think that the impact of these demonstration projects will be on improving interoperability with Canada and Mexican public safety officials?

Could the radios whose communication capabilities are to be improved under the Michigan project be used in the event of, for example, an oil spill in the Great Lakes, a pileup on the Ambassador bridge, or a natural disaster, as well as a terrorist attack or other crime to help Michigan and Canadian police deal with the problems?

Response: The Border Interoperability Demonstration Project (BIDP), formerly known as the International Interoperability Demonstration Project, supports the development of innovative and effective interoperable emergency communications systems and approaches. The seven selected projects will test approaches that involve new technology or an innovative approach to governance, planning, coordination, training, or exercises. The Department of Homeland Security (DHS) selected projects involving multiple communities with varying geography and population densities to test new approaches to enhance interoperable communications capabilities in real-world conditions. The Office of Emergency Communications, within the National Protection

Question#:	3
Topic:	projects
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

and Programs Directorate's Office of Cybersecurity and Communications, will work with selected communities to document lessons learned, capture challenges and successes, and share information with the emergency response community throughout the process.

The goal of these demonstration projects is to improve interoperability for the selected communities. The process of development and implementation will also provide tangible benefit through lessons learned and best practices. These innovative projects and the documented processes will serve as repeatable models for other border communities. Interoperability with Canadian and Mexican public safety officials can be significantly improved, not only in the selected cities, but in all communities that implement projects using the templates and data compiled from the BIDP.

The Michigan project, the Southeast Michigan Border Interoperability Solution, has several objectives, including improving communications for emergency response providers responding to large-scale threats and disasters along the Southeast Michigan/Ontario border area and its connecting waterways. According to Michigan officials, equipment purchased with BIDP funding is intended to be used for all hazards emergency response (e.g., natural disasters, hazmat incidents, crime, terrorist attacks).

67123.275

Question#:	4
Topic:	Canada
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Border Interference Issues with Canada: The congestion in the existing spectrum bands has created a high degree of interference in the U.S.-Canadian border areas. Previous joint agreements have worked to deal with interference issues along the border, for instance, allowing for effective use of the 800 MHz.

If the 700 MHz spectrum is used for a nationwide, interoperable broadband communications network for public safety in the Unites States, we will need to deal with border interference issues in the 700MHz spectrum. For instance, Michigan public safety officials tell us they would only be able to use the future national network in non-border areas due to interference issues, which would be an unacceptable outcome.

What is being done to work out potential interference issues in border areas in the 700 MHz spectrum, since we are aiming to expand the public safety broadband network in that band?

Specifically, what is the status of the international agreements and treaties between the United States and Canada to require Canada to free up some of the 700 MHz spectrum around the border?

Who exactly is working with Canada and Mexico to help facilitate timely and effective international allocation, regulation, and sharing of the 700 MHz spectrum? Is it DHS or the State Department or both?

Response: Responsibility for coordinating 700 MHz Public Safety broadband spectrum within the border zones lies with the Federal Communications Commission (FCC) and Industry Canada (IC). The FCC and IC recently came to agreement on the commercial portion of the 700MHz broadband spectrum, but there has been no formal agreement on the Public Safety portion of the band. The Canadian Government has expressed its intent to develop the Public Safety band to be compatible with U.S. Public Safety broadband efforts.[1]

The Department of Homeland Security and Public Safety Canada are in regular communication about ways to develop or improve interoperability between U.S. and Canadian Public Safety at all levels of government. The Emergency Management

[1] Lucente, Claudio, M.ENG, P.Eng. (2011), *700MHz Spectrum Requirements for Canadian Public Safety Interoperable Mobile Broadband Data Communications*, Defence R&D Canada – Centre for Security Science http://pubs.drdc-rddc.gc.ca/inbasket/mmgreene.110527_1407.DRDC%20CSS%20CR%202011-01.pdf

Question#:	4
Topic:	Canada
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Consultative Group and the Canada-United States Communications Interoperability Working Group will stand up a Communications Interoperability Subcommittee to address issues related to Northern border communications interoperability.

The Department of State leads coordination efforts through the U.S.-Mexico High-Level Consultative Commission (HLCC). The HLCC has identified the update of the existing 2006 Protocol, which includes both the 700 and 800 MHz Public Safety bands, as a key issue for 2011–2013.

Responsibility for these treaty-level agreements and their negotiations resides at the Department of State, with advice and support from the FCC and the National Telecommunications and Information Administration. The Federal Government and Public Safety Canada, including their provincial representatives, also participate in these discussions as necessary.

67123.277

Question#:	5
Topic:	Canada - 2
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Interoperability with Canada: Additional incompatibility issues may disrupt current and planned deployments of public safety systems along the border between the United States and Canada. Since man-made and natural disasters have cross border consequences, first responders on both sides of the border need to be able to communicate and coordinate their responses. The ideal would be a harmonized band of spectrum as well as interoperable emergency communications equipment on each side of the border to enable all first responders to easily communicate.

Is there an expectation that there will eventually be harmonization between the U.S. and Canadian band to enable public safety stakeholders to communicate across jurisdictions? How likely is that outcome?

What steps are being taken to address the problem of interoperability across borders, in addition to the seven international border projects?

Response: The Department of Homeland Security (DHS) and Department of State are working with Public Safety Canada and public safety organizations along the border to identify and develop technology and programs to foster communications interoperability. The Royal Canadian Mounted Police (RCMP) and U.S. Customs and Border Protection (CBP) are working on a test pilot for a system that will allow RCMP officers to communicate directly through their own radio systems with CBP. With a radio over internet protocol interface between the two countries, a high-speed data system will connect command and control centers. This system would eliminate the need for U.S. and Canadian law enforcement officers to share radio equipment or share spectrum to establish radio-to-radio contact for coordination or emergency response. The Border Interoperability Demonstration Project (BIDP) is also being implemented by DHS's National Protection and Programs Directorate's Office of Cybersecurity and Communications' Office of Emergency Communications. BIDP will provide up to $30 million, divided between seven test sites, for innovative communications interoperability along and/or across the borders the United States shares with Canada and Mexico (four along the U.S.-Canada border and three along the U.S.-Mexico border) over the next three years. It is expected that some of the developments from this program will be replicated in many border communities or areas. DHS and Public Safety Canada are in regular communication to develop or improve interoperability between U.S. and Canada public safety at all levels of government. The Emergency Management Consultative Group and the Canada-United States Communications Interoperability Working Group will establish a Communications Interoperability Subcommittee to address issues related to Northern border communications interoperability.

67123.278

Question#:	6
Topic:	D block
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: D-Block: Securing adequate spectrum for and building out a nationwide interoperable public safety broadband network is an important public policy goal that is overdue to be implemented as a recommendation of the 9/11 Commission.

There are now several Congressional proposals that would allocate additional unused spectrum, known as the "D" block, to public safety agencies, with S. 911 proposing using some of the proceeds from commercial auctions of other spectrum to fund the construction of a national interoperable network for first responders.

Public safety officials in Michigan strongly support preserving the D Block spectrum for public safety use. They point out this preservation effort is a once in a lifetime opportunity, because if it is auctioned off for commercial use, that spectrum is gone for good.

Michigan public safety officials have also expressed concern about relying on commercial service, given the crashing of cell phone service in the past when overloaded, and the lack of uniform coverage, especially in rural areas where it is not cost effective. The commercial service contrasts with Michigan's own public safety communications system that has a backup system and provides uniform coverage across the state.

Senator Reid's deficit reduction proposal includes provisions related to the D-Block spectrum. It would reallocate the D Block to public safety and provide $7 billion to finance the building out of the network. Do you have any comments on that proposal and its benefits to first responders?

The funding provided in the Reid proposal to build out the network is $5 billion less than what is in S. 911. What would that reduced funding mean for building out the network in rural areas where there is less existing service?

Response: The Department of Homeland Security strongly agrees with the need to develop a nationwide interoperable Public Safety Broadband Network for our Nation's emergency responders in accordance with the President's National Wireless Initiative. Sufficient funding for this network is critical to ensuring that it has satisfactory coverage and resiliency across the Nation. Reduced funding for the Public Safety Broadband Network would likely shrink its national footprint or limit its functionality.

67123.279

Post-Hearing Questions for the Record
Submitted to Gregory Schaffer
From Senator Mark L. Pryor

"Ten Years After 9/11: Improving Emergency Communications"
July 27, 2011

Question#:	7
Topic:	Goal 2
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: As you mentioned in your testimony, the Office of Emergency Communications is in the process of implementing Goal 2 of the National Emergency Communications Plan. You go on to say that the Goal 2 measurement will allow the Department of Homeland Security to assess emergency communications at the county-level so that Federal and state emergency resources will be provided across the nation to areas "where they are needed most."

Has the Department determined what the criteria will be for distributing Federal and state resources (i.e. grant funding and technical assistance) for counties? If so, what are the criteria?

How will you ensure that rural communities will be given adequate Federal assistance after the Goal 2 assessment?

Response: The National Emergency Communications Plan (NECP) will permit the Department of Homeland Security (DHS) and states to pinpoint the allocation of emergency communications services and resources at the county level. States can use the results generated by the NECP Goals to identify counties most in need of improvement planning, to apply for Federal grants and technical assistance, and to allocate resources accordingly. The Office of Emergency Communications (OEC), within the National Protection and Programs Directorate's Office of Cybersecurity and Communications, will use the results to better target its policy, planning, and support services to address gaps and needs identified during the Goals assessment, including those in counties in rural areas. This applies to OEC's development of Federal grant guidance, the delivery of its technical assistance services, and OEC's support to states' strategic planning activities.

The NECP Goal 2 data will enhance OEC's ability to deliver technical assistance by providing a more accurate picture of current capabilities. To encourage states to address lower performing counties, OEC will provide a report to each Statewide Coordinator showing the county-level results. OEC will ensure prioritization of technical assistance services that address counties that failed to achieve response-level communications and/or address capability areas that were deficient. To ensure rural impact, OEC limits each state to one request for their urban areas and includes scoring criteria on the scope/number of agencies that will be assisted by the technical assistance service.

67123.280

Post-Hearing Questions for the Record
Submitted to Gregory Schaffer
From Senator Susan M. Collins

"Ten Years After 9/11: Improving Emergency Communications"
July 27, 2011

Question#:	8
Topic:	regions
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: We strengthened FEMA regional offices as part of our Katrina reforms in recognition of the fact that major disasters do not usually fit nicely into political boundaries. This is especially true in New England where states are not large. How does OEC work to ensure that not only individual states and localities are well prepared, but that regions are also prepared in the event of a regional disaster?

Response: The Office of Emergency Communications (OEC), a subcomponent of the National Protection and Programs Directorate's Office of Cybersecurity and Communications, contributes to preparedness through programs targeted to improve emergency communications operability and interoperability. This includes the National Emergency Communications Plan (NECP), technical assistance, facilitated statewide workshops, and pilot grants.

OEC also facilitates regional preparedness through its Regional Coordination Program, which consists of a Regional Coordinator (RC) assigned to each of the 10 Federal Emergency Management Agency (FEMA) Regions, including the New England states in Region One. This program supports regional preparedness by strengthening emergency communications capabilities through trusted relationships, collaboration, and knowledge sharing across Federal, state, local, and tribal governments at the regional-levels. RCs support the newly formed Regional Interoperability Councils, which promote communication and collaboration among Statewide Interoperability Coordinators for sharing best practices and establishing interoperable communications solutions with neighboring states and FEMA regions. RCs also regularly participate in the Statewide Interoperability Governing Bodies, Urban Area Security Initiative (UASI) interoperability meetings, and their respective FEMA Regional Emergency Communications Coordination Working Groups to bring together Federal, state, and local governments in their region.

67123.281

Question#:	9
Topic:	exercise
Hearing:	Ten Years After 9/11: Improving Emergency Communications
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: FEMA recently held National Exercise 2011 – which was premised upon an earthquake along the New Madrid Fault in the Midwest. The purpose of this exercise was to coordinate a multi-jurisdictional, integrated response to a national catastrophic event. What information was learned from this exercise regarding communications?

Response: The lessons learned from National Level Exercise 2011 (NLE 11) have yet to be validated, therefore, below are the preliminary observed strengths and areas for improvement identified from the exercise:

Strengths:
- NLE 11 players at all levels of government tested interoperable communications successfully in the following ways:
- Indiana activated its Radio Amateur Civil Emergency Service (RACES) network which allowed local responders to connect with the Indiana State Emergency Operations Center (EOC) in a communications degraded environment.
- Amateur radio operators in Missouri supported local EOCs in establishing alternate interoperable communications with the Missouri State EOC.
- In Arkansas, the State EOC maintained initial communications with the Federal Emergency Management Agency (FEMA) Region VI Office through the Army Military Auxiliary Radio System until normal communications channels were restored later in the exercise. Within a few hours of the event, states impacted by power and communications outages established satellite phone communications with their counties and their FEMA regional offices.
- The interpretation of the Stafford Act to allow funding for private sector partners enabled them to provide communications support.

General areas for improvement:
- While multi-layered communications and Federal communication assets supported the response, there are still critical gaps in the ability to achieve communications after a catastrophic event and ensure that the Federal Government can communicate with populations without power.
- Information technology (IT) issues, such as e-mail capacity limitations and non-standardized e-mail conventions created significant delays in submitting and processing requests for lifesaving and life-sustaining resources.

67123.282

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Defending the Nation Since 9/11:
Successful Reforms and Challenges Ahead at the Department of Homeland Security
Chairman Joe Lieberman
September 7, 2011

Good morning, the hearing will come to order. Thanks for being here. In four days, we will commemorate the tenth anniversary of the attacks of 9/11 and mourn anew for the nearly 3,000 lives that were lost that day at the World Trade Center, the Pentagon, and on Flight 93, which as we all know of course, crashed into a field in Shanksville, Pennsylvania. But we have already quite appropriately begun - and will continue through September 11th - a look back at September 11th to both understand with the clarity of hindsight what that day meant and to evaluate what our government and our people have done since that time.

There's no question that, although we knew it then, we can certainly look back and see now that on that one day we were drawn into a war, which is increasingly global. This is a war that is being fought by Violent Islamist Extremists against most of the rest of the world, including most of the Muslim world. That day, in my own opinion and with the clarity of hindsight, began that war, although Osama bin Laden declared war in 1998 and they had been attacking us for some period of time before then, including the World Trade Center.

But it really began that day. and in the days and months following 9/11/01, we in government set out with an urgent determination to reform the systems that had failed us. I think the more we knew about how September 11th happened, particular through the world of the 9/11 Commission, I came to the conclusion that, though we can never know with certainty, 9/11 was probably preventable.

As we look back at all we've done to respond to our failures on that day, I think if another group of terrorists attempted a similar attack on the United States today, we would prevent it. And that of course gives me great comfort and a sense of great gratitude for all that's been done by so many people in our government to make sure we are more secure than we were on 9/11/01.

We put into place measures that reorganized and reformed our government to prevent another attack on the U.S. I know there are some who are saying that we over reacted to 9/11/01, that it was not just a substantive overreaction, but an expensive overreaction. I don't agree. The most bottom line reality today is that, as we look back over the past 10 years, there has not been another mass casualty attack by Violent Islamist Extremists on the United States since 9/11. I don't think anybody would have predicted that on 9/12/01, but we can say that today, not because our enemies stopped trying, but because our defenses and intelligence have made us more secure. A couple of times we were just plane lucky, as in the glaring cases of the Detroit bomber on Christmas Day and the Times Square bomber, both of whose explosives just didn't go off. If they had, I think we'd be looking back with

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.283

a different sense of the past 10 years. But overall we have been spared another catastrophic terrorist attack like the one on 9/11 just not as a matter of luck, but because of a lot of things people did.

I'm very proud of the role members of this Committee have played in creating these new organizations. The first of course was the cabinet-level Department of Homeland Security (DHS), which we created to lead our efforts to prevent terrorist attacks within the United States. DHS has significantly contributed to our increased national safety. I'm grateful for the report GAO has issued today. Our Committee essentially agrees with it. It's a positive report on the work of the Department of Homeland Security. It points to some work yet to be done, and I think we'd all agree with that, including people at the Department. But the fact is ten years ago, no single agency and no single official were designated to lead the federal government's efforts to prevent terrorism, or for that matter to adequately marshal the resources of the federal government to respond to natural disasters. Today, there is clarity on who is in charge, and who should be coordinating to prepare, respond to and recover from disasters. And that makes a tremendous difference.

I want to thank Deputy Secretary Lute and Gene Dodaro who are both appearing before us today. I am heartened that the report GAO is issuing today concludes overall DHS has implemented most of its key missions and created a foundation that will allow the Department to move aggressively toward its full potential. We appreciate that very much and look forward to the testimony of our witnesses. I will submit the rest of my statement for the record.

Submitted for the Record:

Ten years ago, one of the government's critical weaknesses, as the 9/11 Commission pointed out, was its failure to share information. In the eight and a half years of its existence, DHS has sought to transform information sharing from a limited, need-to-know ethos to sharing across federal agencies and across jurisdictions, with state and local officials who are on the front lines in our fight against terrorism, and with our international partners. Today, there are over 70 fusion centers across the country where federal and state officials sit side-by-side gathering and analyzing information on potential threats together.

One of the areas where our government has made the most progress since 9-11 has been the security of our borders. Before the attacks, three separate cabinet departments were involved in screening individuals and goods coming into the country. And most of the time we didn't know a person intended to travel to the U.S. until they arrived at one of our airports or seaports. Today, we have unified these functions within DHS, and as a result of a number of new programs, we can begin screening and targeting people and goods well before they board an airplane or ship bound for the United States. I recognize that vulnerabilities remain, but it is important to recognize the significant gains that we have made.

Ten years ago, we had an emergency management agency that was simply not equipped to deal with catastrophic disasters, as we found out during Hurricane Katrina. Today, an expanded and strengthened Federal Emergency Management Agency (FEMA) is better prepared and has responded effectively to recent hurricanes, including Irene, which tore through the coastal regions of the Eastern seaboard last week – including my home state of Connecticut - where approximately 830,000 homes and businesses lost power at the height of the storm and the overall economic impact to the state is estimated at $282 million.

Although DHS was created in the wake of the 9/11 terrorist attacks, part of its mission has always been to assist communities in responding to and recovering from disasters of all types – natural or man-made. FEMA has

67123.284

played a significant role in the response to hurricane Irene, and in the weeks and months ahead, people throughout the eastern United States will continue to look to DHS for critical assistance as they work to recover from the devastation caused by major storms.

In the last ten years, we have also increased and substantially improved our screening of passengers and cargo on airplanes bound for or flying within the U.S. We have improved our rail and transit security and the security of our maritime ports. We have begun to implement measures to prevent and detect biological and other WMD attacks. We have better secured chemical plants. And we have ramped up protection of our critical infrastructure, particularly the cyber networks upon which that infrastructure depends. DHS has played an essential role in each of these developments.

The internal workings of the Department have also improved. Melding 200,000 employees and dozens of agencies with different cultures and management policies has not been an easy endeavor. But the Department is better integrated than it has ever been.

None of these achievements, however, mean that we are satisfied. We can still do better, and we must do better. The Department must continue to work every day for greater efficiencies and effectiveness, particularly given the budget climate we are now in.

Today, we are honored to have with us Jane Holl Lute, Department of Homeland Security Deputy Secretary, and Gene Dodaro, Comptroller General of the United States, to discuss the Department's track record over the years – its successes and the challenges yet to be met. The Government Accountability Office (GAO) has issued a new report to stimulate and inform our discussion. I am heartened that the report concludes that overall DHS has implemented key missions and achieved many important goals, creating a foundation that will allow it to continue to mature and reach its full potential. We are grateful, as always, for GAO's deep and careful analysis.

I am particularly interested in our witnesses' thoughts about the budget cuts the Department will certainly face in the coming years. DHS has begun the task of streamlining: It is realizing hundreds of millions of dollars in savings through restrictions on budget components such as employee travel; and by ending ineffective or redundant programs, such as SBINet and the National Security Entry and Exit Registration System. I am concerned, however, that significant additional cuts to DHS's budget, as some have proposed, could reverse many of the homeland security gains that have been achieved since September 11, 2001.

Again, I thank GAO for its important and timely work represented by the report being issued today in conjunction with this hearing. And I especially thank the men and women of DHS for their tireless efforts to protect the American people against the threat of terrorism, respond to natural and manmade disasters, and carry out the Department's many other missions with professionalism, effect, and integrity.

67123.285

Opening Statement of
Ranking Member Senator Susan M. Collins

GAO Report---DHS-Progress Made and Work Remaining in Implementing Homeland Security Missions Ten Years after 9-11

Committee on Homeland Security and Governmental Affairs
September 7, 2011

★ ★ ★

Thank you, Mr. Chairman, for holding today's hearing to review the first eight years of the Department of Homeland Security, whose vital mission is to protect our nation and our people.

After the attacks of September 11, 2001, President Bush established the White House Office of Homeland Security and soon concluded that the nation needed a more unified homeland security structure.

We envisioned a department that would secure our borders, improve the security of transportation and critical infrastructure, meld homeland security intelligence from multiple sources, and work with first responders and law enforcement to deter, detect, prepare for, and respond to terrorist plots. The law establishing the Department of Homeland Security was enacted in November 2002.

Twenty-two entities and approximately 180,000 employees were merged into DHS. Not only was the new department's mission a challenge, so was simply unifying its email systems.

Over the past eight years, the GAO has repeatedly placed the Department on its high-risk list. The GAO has issued about 1,500 recommendations; DHS has adopted only about half of them.

This July, DHS issued a self-administered report card noting considerable progress in achieving the goals set out nearly a decade ago to strengthen our security. When it comes to our homeland security, however, we are only as strong as our weakest link.

This week, we will commemorate the worst attack ever on the United States. In doing so, we must ask ourselves: Are we safer? Or, are we just safer from the tactics the terrorists already have tried?

I think the answer is yes to both. We are far safer than we were on September 10, 2001, but terrorists continue to probe our vulnerabilities and

67123.286

attempt to exploit gaps in our security. We also face increasing threats from homegrown terrorists already within our borders.

Today, GAO concludes that, more than eight years after its creation and 10 years after the September 11 terrorist attacks, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

The examples are many. TSA has strengthened airline passenger pre-screening, but a young man recently was able to fly cross-country without a valid government ID and with an expired boarding pass that was not even in his name. At the other extreme, it troubles many Americans to see TSA screeners putting the very young and the very elderly through intrusive, and in most cases unnecessary, pat downs.

Although DHS has bolstered the security of U.S. borders and identification documents, two Iraqi refugees associated with al Qaeda were recently arrested in Kentucky.

How a known bomb maker, whose fingerprints we have had on file for some time, was able to enter our country on humanitarian grounds remains an unanswered and troubling question.

Are there other Iraqi nationals granted asylum who were involved in attacking our troops? The fact is, we don't know. We still await clear answers from the Administration, which must do more to ensure that all relevant databases are used so we do not let terrorists and criminals into our country.

I am pleased that GAO found that our chemical facilities and seaports are safer, both priorities of mine and this committee.

The GAO indicates that DHS should make improvements in how it shares and manages cyber threat information. That is a key goal of cyber security legislation that Chairman Lieberman, Senator Carper, and I have authored.

The Department has also had its share of management problems. Failures in expensive procurements have cost taxpayers billions of dollars and delayed much-needed technology.

Merging 22 agencies and nearly 180,000 employees is always going to be a challenge. If DHS is to become a true unified department, its employees in headquarters should not remain spread over 70 buildings and 40 sites. The lack of a consolidated headquarters inhibits communication, coordination, and cooperation among DHS components.

I believe there are also efficiencies to be gained by consolidating offices at regional level where there are multiple DHS entities located, a recommendation made by former Homeland Security Secretary Tom Ridge. We should take a look at consolidating field office locations to reduce costs and improve coordination.

As this Committee will soon consider a reauthorization of the Department, it is important to discuss what experts inside and outside of DHS believe has and has not worked. We must answer a fundamental question of whether or not we are safer because of the creation of DHS.

As has been noted often, the terrorists only have to get it right once; DHS and its partners have to be right every time or we will suffer the consequences of an attack. We are much safer than we were on 9-10-01, but we must be tenacious in anticipating the changing tactics of terrorists. As the successful decade-long search for Osama bin Laden proved, America's resolve is a powerful weapon against those who seek to destroy our way of life.

Mr. Chairman, I appreciate the opportunity to review GAO's report with Comptroller General Dodaro and look forward to hearing from Deputy Secretary Lute on how DHS will better fulfill its mission.

Testimony of

Deputy Secretary Jane Holl Lute

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Governmental Affairs

September 7, 2011

Introduction

Chairman Lieberman, Senator Collins, and distinguished Members of the Committee: thank you for the opportunity to appear before you on behalf of the Department of Homeland Security (DHS) to discuss the progress we have made in keeping our Nation safe.

I would also like to thank our many partners in the effort to ensure the safety of our Nation. DHS plays a central role in that effort, but we rely on strong partnerships throughout all levels of government, law enforcement, private industry, and with the public. We view homeland security as a whole of community enterprise, and we are fortunate to have strong partners that help us to meet our mission.

Congress is one of those essential partners. Members of Congress, and particularly this Committee, have played an extraordinary role in creating and equipping DHS and other institutions with both the authorities and the resources necessary to secure our country. You have carried forward the bipartisan spirit that marked the days after 9/11, and have provided DHS with the necessary tools, guidance, and oversight. You have always held us accountable.

Speaking of accountability, we are also thankful for the hard work of our partners at the U.S. Government Accountability Office (GAO). Along with DHS's Office of the Inspector General, GAO's audits help inform us as we mature and grow as an organization. Indeed, overwhelmingly, we tend to agree with GAO recommendations. For example, in the area of management, as a result of our auditors work and our discussions with them, we have put systems in place to ensure that DHS fulfills our missions and that our management lines of business are working.

On this important anniversary, however, we are grateful for the commitment of American citizens, who continue to be our greatest asset in the effort to keep our Nation safe. Since 9/11, countless Americans have stepped up, whether in our military, in our federal agencies including our Department of Homeland Security, and in our states, cities and communities, as first responders, law enforcement officials, and engaged citizens.

Americans know that everyone has a role to play. A commitment to American values is exemplified by the constant refrain that sums up the American call to service: "Send Me." Our challenges are shared challenges, and our successes are shared successes. Our shared goal in securing the homeland was to create a more resilient America, and we have succeeded.

Indeed, the work that has taken place at DHS and around the country since the creation of DHS in 2003 has been remarkable. Former DHS Secretaries Tom Ridge and Michael Chertoff have said that we are now in "Phase III" of this endeavor. While this hearing, and the GAO report, focuses on the successes and challenges of DHS, we actually see this as part of a broader story about the homeland security of the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00664 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.290

DHS Creation and Progress

This hearing comes at a moment of great reflection for our country as we approach the 10th anniversary of the attacks of September 11, 2001.

Following 9/11, the federal government moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, and local capabilities to prepare for, respond to, and recover from threats and disasters at home.

As this Committee knows, a key element of this framework included the creation of DHS, bringing together 22 separate agencies and offices into a single, Cabinet-level Department in March 2003.

Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners have strengthened the homeland security enterprise to better address and defend against dynamic threats.

At DHS, five of our six primary missions align with the goals of the homeland security enterprise:

- Preventing Terrorism and Enhancing Security;
- Securing and Managing our Borders;
- Enforcing and Administering our Immigration Laws;
- Safeguarding and Securing Cyberspace; and
- Ensuring Resilience to Disasters.

Our sixth primary mission captures the operations we perform outside the homeland security enterprise to effectively execute the Department's responsibilities within other federal enterprise missions. In addition to these missions, we have focused on maturing the homeland security enterprise itself. Maturing and strengthening the homeland security enterprise includes enhancing shared awareness of risks and threats, building capable communities, fostering unity of effort, and facilitating innovative approaches and solutions through leading-edge science and technology, while ensuring the efforts aimed at securing the homeland do not diminish privacy, civil rights, or civil liberties.

In each mission area, we have made substantial progress over the past several years, adding new capabilities where none existed before 9/11, fostering greater integration and refinement and coordination of our responsibilities, and broadening the homeland security enterprise to include not just federal departments and entities, but the whole of government as well as our many non-governmental partners.

The results are clear. As a result of the many changes Congress made after 9/11, including the creation of DHS, the restructuring of our Nation's Intelligence Community, and the strengthening of the Federal Emergency Management Agency (FEMA), as well as the contributions and sacrifices of the American people, we are stronger and more resilient today.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00665 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.291

We are a more capable Nation, and a stronger Nation. We are able to detect threats sooner, with better information, and make adjustments more quickly based on continuously updated intelligence. Today we know more about the people seeking to enter our country, the level of risk they pose, and what is needed to prevent potential threats from reaching our shores.

Our borders are stronger, enhanced by more personnel, technology, and infrastructure, as well as stronger partnerships with states and cities, border communities, and our international partners to the North and South.

Our immigration laws, while in need of reform, are being enforced according to common sense priorities we have set, which are to identify and remove criminals and those who are a threat to the American people.

We have also created a framework for securing our cyber systems and networks, and our critical infrastructure, where none previously existed. As part of this effort, we have enhanced our ability to protect federal government networks through better detection, reporting, and threat mitigation. We have engaged cyber-users at all levels, public and private, in our shared protection. And we have broadened our partnership with the private sector to protect our critical infrastructure, and established a new regulatory framework to protect high-risk chemical facilities.

We have built a more ready and resilient Nation that is able to confront major disasters in our states, cities, and communities. We have helped frontline responders become more equipped, better trained, and more unified under a new National Response Framework and Incident Command System. We have improved emergency communications. And we have provided billions of dollars in grants to support our Nation's first responders.

We have continued to integrate DHS, advancing the work that began more than eight years ago to refashion our homeland security enterprise and engage a full set of partners in the protection of our Nation.

Finally, we have represented in our programs and activities the Department's commitment to the idea that core civil rights values – liberty, fairness, and equality under the law – are a vital part of America, and that it is these values that also provide a bulwark against those who threaten our safety and security.

Nevertheless, we know that we must continue to improve. As the threat against us continues to evolve, so do we. Today, then, is an opportunity to talk about some of our progress, which the GAO notes in its report, and also address some of the areas where there is more work to be done.

Preventing Terrorism and Enhancing Security

Our country has made significant progress in securing the Nation from terrorism since the September 11, 2001 attacks. This work has included constant enhancements and evolutions to our layered approach to security through the development of formalized terrorism risk

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00666 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.292

assessments, deployment of new technology, expanded data analysis capabilities, and applying intelligence to our security measures in near real time.

To understand the landscape of potential chemical, biological, radiological or nuclear (CBRN), terrorist threats, the DHS Science and Technology (S&T) Directorate has developed a first-of-its kind capability to provide DHS components as well as external federal partners with a systematic, science-based, formal assessment of CBRN terrorism risk to the Homeland.

Prior to 9/11, screening of passengers coming to the United States was limited to the Department of State visa process and the inspection of a person by an immigration officer at the port of entry. Provision of advance passenger information by airlines was voluntary and often inconsistent.

Over the past ten years, we have significantly adapted and enhanced our ability to detect threats, building a layered, risk-based system that includes a full range of identification verification measures – from visa application checks and biometric identification to the receipt of advanced passenger information and the full implementation of Secure Flight, a program that enables DHS to prescreen 100 percent of passengers on flights flying to, from, or within the United States against government watch lists.

With support from international partners and the aviation industry, we have implemented pre-departure programs for U.S. bound flights as well as enhanced security measures to strengthen the safety and security of all passengers.

These new measures, which cover 100 percent of passengers traveling by air to the United States, utilize continuously updated, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

Prior to 9/11, there also was no advance screening of passengers seeking admission under the Visa Waiver Program (VWP), which enables nationals of 36 designated countries to travel to the United States for stays of 90 days or less without obtaining a visa. In 2008, DHS implemented the Electronic System for Travel Authorization (ESTA) to screen prospective VWP travelers against several databases, including the terrorist watchlist; lost and stolen passports; visa revocations; previous VWP refusals; and public health records.

In addition, prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today, all checked and carry-on baggage aboard aircraft is screened for explosives. Increased levels of frontline security personnel at the passenger checkpoints and new technologies have significantly enhanced security as well. Today, TSA personnel serve on the frontlines at over 450 U.S. airports.

We also have taken significant action to counter the threat of nuclear, biological, and radiological weapons or materials entering the United States. When the Department was formed, we scanned only 68 percent of arriving trucks and passenger vehicles along the Northern border for radiological and nuclear threats. No scanning systems were deployed to the Southwest border and only one was deployed to a seaport. Today, these systems scan 100 percent of all

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00667 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.293

containerized cargo and personal vehicles arriving in the U.S. through land border ports of entry, as well as over 99 percent of arriving sea containers.

Since the anthrax attacks 10 years ago, we also have made great strides in protecting the Nation from, and preparing federal, state, and local governments to respond to biological attacks. In 2003, the Department stood up the BioWatch system—a federally-managed, locally-operated, nationwide environmental surveillance system designed to detect the intentional release of aerosolized biological agents which is currently operational in approximately 30 cities and states.

The terrorist threats facing the United States have evolved significantly over the last decade, and continue to evolve. In addition to the direct threats from al-Qa'ida, foreign terrorist groups affiliated with al-Qa'ida, as well as individual violent extremist thought leaders, are seeking to recruit or inspire individuals in the Homeland to carry out attacks with little or no warning.

The threat posed by violent extremism is neither constrained by international borders nor limited to any single ideology. Groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the Homeland. Increasingly sophisticated use of the Internet, mainstream and social media, and information technology by violent extremists adds an additional layer of complexity.

To counter violent extremism (CVE), DHS is working with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to potential terrorist activity within the United States, and the best ways to mitigate or prevent that activity. Our approach to CVE emphasizes the strength of local communities.

We begin with the premise that well-informed and -equipped families, communities, and local institutions represent the best defense against terrorist ideologies. And while our primary purpose is to prevent a terrorist and violent extremist attack by an individual or group recruited by a violent extremist organization, or inspired by an extremist ideology, we also support strong and resilient communities as important ends themselves.

To implement this approach, we are working closely with our federal and international partners, as well as our many partners at the community, state, local, and tribal levels across the country. We are an important partner in supporting the National Strategy on Empowering Local Partners to Prevent Violent Extremism, which President Obama released on August 3, 2011.

Securing and Managing our Borders

Protecting our Nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to homeland security, as well as economic prosperity.

To meet this responsibility, we have deployed unprecedented levels of personnel, technology, and resources to the Southwest border. At the same time, we have made critical security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure while also strengthening efforts to increase the security of the Nation's maritime borders.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00668 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.294

Today, the Border Patrol has more staff than at any time in its 87-year history. Along the Southwest border, DHS has increased the number of civilian boots on the ground from approximately 9,100 Border Patrol agents in 2001 to more than 17,700 today.

Under the Southwest Border Initiative, we have doubled the number of personnel assigned to Border Enforcement Security Task Forces (BESTs), which leverage federal, state, local, tribal and foreign law enforcement and intelligence resources in an effort to identify, disrupt, and dismantle transnational criminal organizations that seek to exploit vulnerabilities along the U.S. borders and threaten the overall safety and security of the American public.

We have increased the number of U.S. Immigration and Customs Enforcement (ICE) intelligence analysts along the border focused on cartel violence; quintupled deployments of Border Liaison Officers to work with their Mexican counterparts; begun screening 100 percent of southbound rail shipments for illegal weapons, drugs, and cash; and expanded Unmanned Aircraft System (UAS) coverage to the entire Southwest border. There were no deployments of UASs along the Southwest border prior to 9/11.

Further, the $600 million supplemental funding requested by the Administration and passed by Congress in 2010, with nearly $400 million targeted for DHS, is enabling us to continue to add technology, personnel, and infrastructure to the Southwest border. These resources include 1,000 additional Border Patrol Agents; 250 new U.S. Customs and Border Protection officers at U.S. ports of entry; 250 new ICE agents focused on transnational crime; improved tactical communications systems; two new forward operating bases to improve coordination of border security activities; and additional CBP UASs.

While this work is not yet complete, every key metric currently available shows that these border security efforts are producing significant results. Illegal immigration attempts, as measured by Border Patrol apprehensions, have decreased 36 percent in the past two years, and are less than one third of what they were at their peak. Seizures of drugs, weapons and currency have increased across the board. The S&T Directorate continues to improve current detection technologies and look at advanced sensors and systems for CBP and Coast Guard in order to provide a more effective and cost efficient means for securing our land and maritime borders.

In July 2011, the Obama Administration also released its most recent National Southwest Border Counternarcotics Strategy, which provides the Administration's overarching framework to address the threats posed by the illicit narcotics trade. And DHS has forged historic agreements with the Department of Justice (DOJ), increasing coordination between ICE and the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Drug Enforcement Administration (DEA) on important Southwest border issues such as combating arms trafficking, bolstering information sharing and providing ICE agents the authority to work on important drug trafficking cases.

In addition, we have signed numerous bilateral agreements and declarations to bolster and deepen collaboration with Mexico in the areas of enforcement, planning, information and intelligence sharing, joint operations, and trade facilitation along the Southwest border.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00669 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.295

On our Northern border, we continue to invest in personnel, technology, and infrastructure, and to strengthen cooperation with federal, state/provincial, tribal, and private sector partners on both sides of the border. These achievements have resulted in a more secure Northern border that facilitates legitimate travel and trade.

Currently, CBP has more than 2,200 Border Patrol agents on the Northern border, a 500 percent increase since 9/11. CBP also has nearly 3,700 CBP officers managing the flow of people and goods across ports of entry and crossings along the Northern border.

The Department has also continued to deploy technology along the Northern border, including thermal camera systems, Mobile Surveillance Systems, Remote Video Surveillance Systems, and long-range CBP Predator-B unmanned aircraft patrols. In February 2011, President Obama and Canadian Prime Minister Harper announced a landmark "Shared Vision for Perimeter Security and Economic Competitiveness" that sets forth how the two countries will manage shared homeland and economic security in the 21st century. This shared vision, or "Beyond the Border," continues to protect individual privacy and civil liberties while securing the flows of trade and travel that strengthens North American perimeter security and the overall economy.

The U.S. Coast Guard continues to work with other federal, state, local and tribal partners to enhance security along the U.S. maritime border and uses interagency partnerships and international bilateral agreements to accomplish this mission. The Coast Guard leverages its unique maritime security authorities, capabilities and partnerships to mitigate risk and improve security in our domestic ports, on the high seas, and in ports abroad through a layered security approach. Closer to shore, the Coast Guard patrols our ports, conducts vessel escorts, and inspects vessels and facilities.

With respect to identity document security, DHS also has taken significant steps to strengthen security, reduce fraud and improve the reliability and accuracy of personal identification documents while enhancing privacy safeguards. For example, we have fundamentally transformed the way travelers enter the United States from within the Western Hemisphere through implementation of the Western Hemisphere Travel Initiative (WHTI) and from other countries around the world through the VWP, Visa Security Program and US-VISIT biometric identity and verification process.

Prior to the implementation of WHTI, there was no standard documentary requirement for U.S. or most Canadian citizens to enter the United States from within the Western Hemisphere; travelers could present any one of numerous documents or simply make an oral declaration of citizenship. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases. Today, due to WHTI, the national query rate is over 97 percent.

Enforcing and Administering our Immigration Laws

What we do to protect our borders is inseparable from immigration enforcement in the interior of our country, and both are critical to an effective immigration system.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00670 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.296

Our approach to immigration enforcement has focused on identifying criminal aliens and those who pose the greatest risk to our communities, and prioritizing them for removal. In addition, we have worked to ensure that employers have the tools they need to maintain a legal workforce, and face penalties if they knowingly and repeatedly violate the law. And we have made significant changes to our immigration detention system, to recognize the basic differences between immigration violators – from non-violent aliens to hardened, violent criminals and gang members – and house them accordingly in order to optimize the safety and security of other detainees and the facilities' staff.

Like our actions at the border, our interior enforcement efforts are achieving major results. In Fiscal Years 2009 and 2010, ICE removed more illegal immigrants from our country than ever before, with more than 779,000 removals nationwide in the last two years. Most importantly, more than half of those aliens removed last year – upwards of 195,000 – were convicted criminals, the most ever removed from our country in a single year.

We also have stepped up our efforts to target employers who repeatedly and egregiously break the law, last year arresting a record number of employers who knowingly hire illegal aliens. ICE has significantly expanded its use of I-9 audits, which are used to investigate employers suspected of employing illegal aliens. Since January 2009, ICE has audited more than 3,600 employers suspected of employing unauthorized aliens, debarred more than 260 companies and individuals, and imposed approximately $56 million in financial sanctions – more than the total amount of audits and debarments than during the entire previous administration.

We also have strengthened the efficiency and accuracy of E-Verify – our on-line employment verification system managed by U.S. Citizenship and Immigration Services (USCIS). More than 249,000 employers are enrolled in E-Verify, representing more than 857,000 locations. More than 1,300 new employers enroll each week and the number of employers enrolled in E-Verify has more than doubled each fiscal year since 2007.

To combat the growing problem of smuggling and trafficking, we also have continued to conduct targeted enforcement operations while launching national public awareness campaigns, including in Central and South America, to shine a spotlight on this unconscionable crime. DHS also launched the Blue Campaign to Combat Human Trafficking, a national initiative focused on protection, prevention, and prosecution.

Of course, our country is a nation of immigrants, and we must remain open and welcoming to new immigrants while supporting their integration into our society. USCIS has taken a number of actions to improve its ability to meet these goals. By streamlining and modernizing operations, USCIS is now processing applications for naturalization and other critical immigration benefits more rapidly, meeting or exceeding performance goals. As a customer-focused agency, USCIS also has taken steps to improve one of its primary interfaces with the public through its website: www.uscis.gov.

USCIS also has made security enhancements to some of its key identity documents to prevent counterfeiting, obstruct tampering, and facilitate quick and accurate authentication. And USCIS continues to enhance fraud detection and national security capabilities to ensure that immigration

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00671 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.297

benefits are not granted to individuals who pose a threat to national security. For example, USCIS has embedded Fraud Detection and National Security officers in nine other government agencies to increase information sharing and collaboration efforts that enhance law enforcement and intelligence operations.

Finally, USCIS has continued to naturalize thousands of new Americans each year, including record numbers of members of our Nation's Armed Forces. In FY 2010, USCIS granted citizenship to 11,146 members of the U.S. Armed Forces at ceremonies in the United States and 22 countries abroad. This figure represents the highest number of service members naturalized in any year since 1955.

These improvements to our legal immigration system, coupled with our efforts to secure the border and enforce immigration laws in the interior, are producing significant results. We know that more is required to fully address our Nation's immigration challenges. Ultimately, Congress needs to take up reforms to our immigration system to address long-standing, systemic problems with our Nation's immigration laws.

Safeguarding and Securing Cyberspace

Today's threats to cybersecurity require the engagement of our entire society—from government and law enforcement to the private sector and importantly, members of the public— to block malicious actors while bolstering defensive capabilities.

DHS is responsible for protecting the federal executive branch civilian agencies, and assisting in the protection of the Nation's critical infrastructure and critical information systems where the government maintains sensitive information and which provide services to the American people and support the financial services, energy, and defense industries.

Over the past ten years, DHS has made significant strides in enhancing the security of the Nation's critical physical infrastructure as well as its cyber infrastructure and networks. In October 2010, DHS and the Department of Defense (DOD) signed a Memorandum of Agreement to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks. The Agreement embeds DOD cyber analysts within DHS and sends DHS privacy, civil liberties, and legal personnel to DOD's National Security Agency to strengthen the Nation's cybersecurity posture and ensure the protection of fundamental rights.

In partnership with the private sector, the U.S. Computer Emergency Readiness Team (US-CERT) continues to take proactive measures to stop possible threats by developing and sharing standardized threat indication, prevention, mitigation, and response information products with its governmental and private sector partners.

DHS also has developed the first-ever National Cyber Incident Response Plan in September 2010 to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00672 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.298

In October 2009, DHS also opened the new National Cybersecurity and Communications Integration Center (NCCIC) —a 24-hour, DHS-led coordinated watch and warning center to serve as the Nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture.

DHS also utilizes the National Cybersecurity Protection System, of which the EINSTEIN intrusion detection system is a key component, to protect the dot-gov domains. When fully deployed, the latest version of the EINSTEIN system, the first version of which was deployed in 2004, will help block malicious actors from accessing federal executive branch civilian agencies. At the same time, DHS is working closely with those agencies to bolster their defensive capabilities.

Additionally, as part of the Comprehensive National Cybersecurity Initiative, DHS is working to reduce and consolidate the number of external connections that federal agencies have to the Internet through the Trusted Internet Connection (TIC) initiative. And to meet our future workforce needs, DHS is also building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to Critical Infrastructure and Key Resources (CIKR).

Finally, DHS is committed to increasing public awareness about cybersecurity and empowering individuals and enterprises across cyber networks to enhance their own security operations. In 2010, the Department launched the *"Stop. Think. Connect."* public cybersecurity awareness campaign to increase public understanding of cyber threats and promote simple steps the public can take to increase their safety and security online. Additionally, DHS S&T co-sponsors national and regional cybersecurity competitions at the high school and collegiate levels, to educate young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts.

Ensuring Resilience To Disasters

DHS provides the coordinated, comprehensive Federal response in the event of a terrorist attack, natural disaster or other large-scale emergency while working with Federal, state, local, and private sector partners to ensure a swift and effective recovery effort. Over the past ten years, we have worked to strengthen our Nation's ability to prepare for, protect against, respond to, recover from and mitigate major emergencies and disasters of all kinds, at all levels.

To strengthen emergency preparedness and response planning, we issued the National Response Framework in January 2008, which builds on predecessor plans that did not exist prior to 9/11. We also revised the National Incident Management System in December 2008.

We have substantially strengthened FEMA, giving it – with the help and guidance of this Committee – a more effective structure, better tools and technology, new logistics capabilities, more effective sheltering planning, and a "forward leaning" posture that pushes more assets and resources into the field in advance of a disaster when capabilities of the States are overwhelmed.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00673 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.299

To support state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies, we have awarded more than $31 billion in preparedness grant funding since 2003. This funding is based on risk to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism.

In addition, to enhance emergency and interoperable communications, we developed the National Emergency Communications Plan in coordination with more than 150 public safety practitioners at all levels and across responder disciplines. The National Emergency Communications Plan is our Nation's first nationwide strategic plan to improve emergency communications and drive progress at all levels of government. We have also made over $4 billion in grants for interoperable communications available and increasingly aligned them with national and state plans.

DHS Transformation and Integration

Finally, we have taken significant steps to create a unified and integrated Department, focusing on accountability, transparency and leadership development to enhance our mission performance. We are implementing a comprehensive, strategic management approach to enhance the people, structures, and processes needed to meet our mission. This approach integrates and aligns our business functions at the Departmental and Component levels and is focused on three key elements:

1. Acquisition Enhancement: Improving upon the current Department process and procedures – particularly the "front end" requirements and the "back end" program management to minimize risk, encourage fiscal responsibility, and execution across the acquisition life-cycle.

2. Financial Enhancement: Improving our financial systems and capabilities in both the management directorate and the components.

3. Human Capital Management Enhancement: Making sure we have the right people in the right positions at the right time, with the proper workforce balance between DHS and contract employees.

DHS has a strong commitment to effective acquisition management. In August, 2007, we established the Acquisition Program Management Division to help strengthen acquisition management within DHS. In the future we will establish an Investment Review Board to oversee the status of all acquisition investments. We also have revised our acquisition management oversight policies to include more detailed guidance to inform our acquisition decisions.

We are also firmly committed to strengthening Department-wide financial management, and we have made progress in this area. The results of our FY 2010 financial annual audit have demonstrated steady progress toward sound financial results.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00674 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.300

For example, we have reduced the number of material weakness conditions over financial reporting by half since FY 2005. We also have formalized Department-wide uniform processes and procedures to strengthen accounting and financial reporting.

To meet human capital needs, we issued our Workforce Strategy for Fiscal Years 2011-2016 in December 2010, which contains the Department's workforce goals, objectives, and performance measures for human capital management. We are also developing component operational plans and tracking those plans against a common set of performance measures. In addition, we have developed a diversity council, among other initiatives, to ensure we have a workforce that reflects the diversity of America.

Conclusion

The guiding philosophy behind the homeland security enterprise – shared responsibility – means that we share both responsibility and success among our many partners in the homeland security effort.

The complexity of this challenge, and its import, not only to the United States but to nations that look to us for guidance, makes it essential that we succeed. It is only through a whole of community approach that we can build the necessary capabilities, countermeasures, and sustained public and private sector engagement required to keep our country safe in the face of evolving threats, and to build the resilience needed to bounce back from threats, challenges, and setbacks.

This Committee has been instrumental to our ability to achieve our mission thus far, and your partnership and support will be essential in the future. We look forward to continuing our work with you, and we remain grateful for all that you have done to help us succeed over the past eight years and since 9/11.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00675 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.301

United States Government Accountability Office

GAO

Testimony
Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 7, 2011

DEPARTMENT OF HOMELAND SECURITY

Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

Statement of Gene L. Dodaro
Comptroller General of the United States

U.S. Government Accountability Office
GAO 90 YEARS 1921-2011
ACCOUNTABILITY * INTEGRITY * RELIABILITY

GAO-11-919T

67123.302

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-11-919T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate.

September 7, 2011

DEPARTMENT OF HOMELAND SECURITY

Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

Why GAO Did This Study

The terrorist attacks of September 11, 2001, led to profound changes in government agendas, policies and structures to confront homeland security threats facing the nation. Most notably, the Department of Homeland Security (DHS) began operations in 2003 with key missions that included preventing terrorist attacks from occurring in the United States, reducing the country's vulnerability to terrorism, and minimizing the damages from any attacks that may occur. DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. Since 2003, GAO has issued over 1,000 products on DHS's operations in such areas as border and transportation security and emergency management, among others. As requested, this testimony addresses DHS's progress and challenges in implementing its homeland security missions since it began operations, and issues affecting implementation efforts. This testimony is based on a report GAO is issuing today, which assesses DHS's progress in implementing its homeland security functions and work remaining.

What GAO Recommends

While this testimony contains no new recommendations, GAO previously made about 1,500 recommendations to DHS. The department has addressed about half of them, has efforts underway to address others, and has taken additional action to strengthen its operations. In commenting on GAO's report upon which this testimony is based, DHS stated that the report did not address all of DHS's activities. The report was based on prior work, which GAO reflected throughout the report.

View GAO-11-919T or key components. For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

Since it began operations in 2003, DHS has implemented key homeland security operations and achieved important goals and milestones in many areas to create and strengthen a foundation to reach its potential. As it continues to mature, however, more work remains for DHS to address gaps and weaknesses in its current operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. DHS's accomplishments include developing strategic and operational plans; deploying workforces; and establishing new, or expanding existing, offices and programs. For example, DHS

- issued plans to guide its efforts, such as the Quadrennial Homeland Security Review, which provides a framework for homeland security, and the National Response Framework, which outlines disaster response guiding principles;
- successfully hired, trained, and deployed workforces, such as a federal screening workforce to assume security screening responsibilities at airports nationwide; and
- created new programs and offices to implement its homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to help coordinate efforts to address cybersecurity threats.

Such accomplishments are noteworthy given that DHS has had to work to transform itself into a fully functioning department while implementing its missions—a difficult undertaking that can take years to achieve. While DHS has made progress, its transformation remains high risk due to its management challenges. Examples of progress made and work remaining include:

Border security. DHS implemented the U.S. Visitor and Immigrant Status Indicator Technology program to verify the identities of foreign visitors entering and exiting the country by processing biometric and biographic information. However, DHS has not yet determined how to implement a biometric exit capability and has taken action to address a small portion of the estimated overstay population in the United States (individuals who legally entered the country but then overstayed their authorized periods of admission). DHS also deployed infrastructure to secure the border between ports of entry, including more than 600 miles of fencing. However, DHS experienced schedule delays and performance problems with the Secure Border Initiative Network, which led to the cancellation of this information technology program.

Aviation security. DHS developed and implemented Secure Flight, a program for screening airline passengers against terrorist watchlist records. DHS also developed new programs and technologies to screen passengers, checked baggage, and air cargo. However, DHS does not yet have a plan for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements, a mechanism to verify the accuracy of data to help ensure that air cargo screening is being conducted at reported levels, or approved technology to screen cargo once it is loaded onto a pallet or container.

Emergency preparedness and response. DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00677 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.303

based preparedness, and a Target Capabilities List to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS is also finalizing a National Disaster Recovery Framework. However, DHS needs to strengthen its efforts to assess capabilities for all-hazards preparedness, and develop a long-term recovery structure to better align timing and involvement with state and local governments' capacity. DHS should also improve the efficacy of the grant application process by mitigating duplication or redundancy within the various preparedness grant programs.

Chemical, biological, radiological and nuclear (CBRN) threats. DHS assessed risks posed by CBRN threats and deployed capabilities to detect CBRN threats. However, DHS should work to improve its coordination of CBRN risk assessments, and identify monitoring mechanisms for determining progress made in implementing the global nuclear detection strategy.

GAO's work identified three themes at the foundation of DHS's challenges.

Leading and coordinating the homeland security enterprise. DHS has made important strides in providing leadership and coordinating efforts among its stakeholders. However, DHS needs to take additional action to forge effective partnerships and strengthen the sharing and utilization of information, which has affected its ability to effectively satisfy its missions. For example, the expectations of private sector stakeholders have not been met by DHS and its federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. In 2005, GAO designated information sharing for homeland security as high risk because the federal government faced challenges in analyzing and sharing information in a timely, accurate, and useful way.

Implementing and integrating management functions for results. DHS has enhanced its management functions, and has plans in place to further strengthen the management of the department for results. However, DHS has not always effectively executed or integrated these functions. In 2003, GAO designated the transformation of DHS as high risk because DHS had to transform 22 agencies into one department. DHS has demonstrated strong leadership commitment and begun to implement a strategy to address its management challenges. However, these challenges have contributed to schedule delays, cost increases, and performance problems in a number of programs aimed at delivering important mission capabilities, such as container security technologies. DHS also faced difficulties in deploying some technologies that meet defined requirements. Further, DHS does not yet have enough skilled personnel to carry out activities in various areas, such as acquisition management; and has not yet developed an integrated financial management system, impacting its ability to have ready access to reliable information for informed decision making.

Strategically managing risks and assessing homeland security efforts. Forming a new department while working to implement statutorily mandated and department-initiated programs and responding to evolving threats, was, and is, a significant challenge facing DHS. Key threats have impacted DHS's approaches and investments. It is understandable that these threats had to be addressed immediately as they arose. However, limited strategic and program planning by DHS and limited assessment to inform approaches and investment decisions have contributed to programs not meeting strategic needs in an efficient manner.

Given DHS's leadership responsibilities in homeland security, it is critical that its programs are operating as efficiently and effectively as possible, are sustainable, and continue to mature to address pressing security needs. Eight years after its creation and 10 years after September 11, 2001, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00678 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.304

Chairman Lieberman, Ranking Member Collins, and Members of the Committee:

I am pleased to be here today to discuss our work on progress made by the Department of Homeland Security (DHS) and work remaining in implementing its homeland security missions since it began operations in March 2003. The nation is about to pass the 10-year anniversary of the September 11, 2001, terrorist attacks. The events of that day led to profound changes in government agendas, policies, and structures to confront homeland security threats facing the nation. This milestone provides an opportunity to reflect on the progress DHS has made since its establishment and challenges it has faced in implementing its missions, as well as to identify issues that will be important for the department to address as it moves forward, based on work we have completed on DHS programs and operations in key areas.

DHS was established with key missions that include preventing terrorist attacks from occurring within the United States, reducing U.S. vulnerability to terrorism, minimizing resulting damages, and helping the nation recover from any attacks that may occur. DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. We have evaluated numerous departmental programs since DHS began its operations, and issued more than 1,000 reports and congressional testimonies in areas such as border security and immigration, transportation security, and emergency management, among others.

We have made approximately 1,500 recommendations to DHS designed to strengthen its operations, such as to improve performance measurement efforts, strengthen management processes, enhance coordination and information sharing, and increase the use of risk information in planning and resource allocation decisions, as well as to address gaps and challenges in its mission operations that have affected DHS's implementation efforts. DHS has implemented about half of these recommendations, has actions underway to address others, and has taken additional steps to strengthen its mission activities.

However, we reported that the department has more to do to ensure that it conducts its missions efficiently and effectively, while simultaneously preparing to address future challenges that face the department and the nation. Addressing these issues will likely become increasingly complex as domestic and world events unfold, and will be particularly challenging in light of the current fiscal environment and constrained budgets.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00679 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.305

In 2003, we designated the implementation and transformation of DHS as high risk because it represented an enormous undertaking that would require time to achieve in an effective and efficient manner.[1] Additionally, the components that merged to form DHS already faced a wide array of existing challenges, and any DHS failure to effectively carry out its mission could expose the nation to potentially serious consequences. The area has remained on our high-risk list since 2003.[2] Our prior work on mergers and organizational transformations, undertaken before the creation of DHS, found that successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take years to achieve.[3]

In 2007, we reported on progress made by DHS in implementing its mission and management functions by assessing actions DHS took to achieve performance expectations within each function.[4] We reported that DHS made progress in implementing all of its mission and management functions since it began operations, but progress among the areas varied significantly. For example, we reported that DHS made more progress in implementing its mission functions than its management functions. We also reported that DHS generally had not established

[1] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003). In addition to this high-risk area, DHS has responsibility for other areas we have designated as high risk. Specifically, in 2005 we designated information sharing for homeland security as high risk, involving a number of federal departments including DHS, and in 2006, we identified the National Flood Insurance Program as high risk. Further, in 2003 we expanded the scope of the high-risk area involving federal information security, which was initially designated as high-risk in 1997, to include the protection of the nation's computer-reliant critical infrastructure.

[2] GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).

[3] See GAO, *Highlights of a GAO Forum: Mergers and Transformations: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*, GAO-03-293SP (Washington, D.C.: Nov. 14, 2002), and *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

[4] GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007). We defined performance expectations as a composite of the responsibilities or functions—derived from legislation, homeland security presidential directives and executive orders, DHS planning documents, and other sources—that the department was to achieve or satisfy in implementing efforts in its mission and management areas. The performance expectations were not intended to represent performance goals or measures for the department.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00680 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.306

quantitative goals and measures for assessing its performance and, as a result, we could not assess where along a spectrum of progress DHS stood in achieving its missions. Subsequent to the issuance of this report, DHS continued to take action to strengthen its operations and the management of the department, including enhancing its performance measurement efforts. At the request of this Committee, following the issuance of our report, we provided DHS with feedback on the department's performance goals and measures as DHS worked to better position itself to assess its results. Based on its internal review efforts and our feedback, DHS took action to develop and revise its performance goals and measures in an effort to strengthen its ability to assess its outcomes and progress in key mission areas. For fiscal year 2011, DHS identified 85 strategic measures for assessing its progress in achieving its Quadrennial Homeland Security Review (QHSR) missions and goals.[5] The department plans to report on its results in meeting established targets for these new measures at the end of the fiscal year.

In February 2010, DHS issued its first QHSR report, outlining a strategic framework for homeland security to guide the activities of the department and its homeland security partners, including federal, state, local, and tribal government agencies; the private sector; and nongovernmental organizations. The report identified five homeland security missions—Preventing Terrorism and Enhancing Security, Securing and Managing Our Borders, Enforcing and Administering Our Immigration Laws, Safeguarding and Securing Cyberspace, and Ensuring Resilience to Disasters—and goals and objectives to be achieved within each mission. In addition, in July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR), a departmentwide assessment to align DHS's programmatic activities, such as investigating drug smuggling and

[5] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010). The Implementing Recommendations of the 9/11 Commission Act required that beginning in 2009, and every 4 years thereafter, DHS conduct a quadrennial review that provides a comprehensive examination of the homeland security strategy of the United States. Pub. L. No. 110-53, § 2401(a), 121 Stat. 266, 543-45 (2007) (codified at 6 U.S.C. § 347).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00681 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.307

inspecting cargo at ports of entry, and its organizational structure to the missions and goals identified in the QHSR.[6]

My statement is based on a report we are issuing today assessing DHS's programs and operations.[7] As requested, the report and my statement address the progress made by DHS in implementing its homeland security missions since it began operations, remaining work, and crosscutting and management issues that have affected DHS's implementation efforts.

The report is based on our work on DHS since it began operations, supplemented with work completed by the DHS Office of Inspector General (IG), with an emphasis on work completed since 2008 to reflect recent work, and updated information and documentation provided by the department in July and August 2011. It is also based on our ongoing work on some DHS programs for various congressional committees, as noted throughout the report. For this ongoing work, as well as updated information provided by DHS, we examined program documentation and interviewed agency officials, among other things. This statement highlights key, recent work at DHS, but does not address all products we and DHS IG issued related to the department, nor does it address all of DHS's homeland security-related activities and efforts. To determine what progress DHS has made in implementing its mission functions and what work, if any, remains, we identified 10 DHS functional areas, which we define as categories or areas of DHS's homeland security responsibilities. These functional areas are based on those areas we identified for DHS in our August 2007 report on DHS's progress in implementing its mission and management functions, and our analysis of DHS's QHSR and budget documents, such as its congressional budget justifications.[8] These areas include: (1) aviation security; (2) chemical, biological, radiological, and nuclear (CBRN) threats; (3) critical infrastructure protection—physical

[6] DHS, *Bottom-Up Review Report* (Washington, D.C.: July 2010). As a result of the BUR, DHS acknowledged that it had complementary department responsibilities and capabilities, which it subsequently formalized in a sixth mission published in the fiscal year 2010-2012 Annual Performance Report—"Providing Essential Support to National and Economic Security"—to fully capture the scope of DHS's missions.

[7] GAO, *Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11*, GAO-11-881 (Washington, D.C.: Sept. 7, 2011).

[8] GAO-07-454.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00682 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.308

assets; (4) surface transportation security; (5) border security; (6) maritime security; (7) immigration enforcement; (8) immigration services; (9); critical infrastructure protection—cyber assets; and (10) emergency preparedness and response.[9] To identify sub-areas within these functional areas, we identified performance expectations, which we define as composites of the responsibilities or functions that the department is to achieve or satisfy based on our analysis of requirements, responsibilities, and goals set for the department by Congress, the administration, and DHS itself and its components. In particular, we used expectations identified in our August 2007 report as a baseline, and updated, or added to, these expectations by analyzing requirements and plans set forth in homeland security-related laws, presidential directives and executive orders, national strategies, and DHS's and components' strategic plans and documents. We then aligned our functional areas to the five QHSR missions based on our review of the QHSR and BUR reports and DHS's fiscal year 2012 budget documents.

To identify key areas of progress and work that remains in each functional area, as well as crosscutting issues that have affected DHS's implementation efforts, we examined our and the DHS IG's past reports. We selected key work that we and the DHS IG have completed related to the functional areas, sub-areas, and crosscutting issues. We examined the methodologies used by the DHS IG in its reports, including reviewing the scope, methodological steps, and limitations. We determined that the DHS IG reports were sufficiently reliable for the purposes of our report to provide examples of, and to supplement our work on, DHS's progress and work remaining. We identified crosscutting issues based on analysis of our work in each functional mission area to determine common themes that have affected DHS's implementation efforts across the various mission areas. We conducted this performance audit from April 2011 through September 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan

[9] We focused these mission areas primarily on DHS's homeland security-related functions. We did not consider the Secret Service, domestic counterterrorism or intelligence activities because (1) we and the DHS IG have completed limited work in these areas; (2) there are few, if any, requirements identified for the Secret Service's mission and for DHS's role in domestic counterterrorism and intelligence (the Department of Justice serves as the lead agency for most counterterrorism initiatives); and (3) we address DHS actions that could be considered part of domestic counterterrorism and intelligence in other areas, such as aviation security, critical infrastructure protection, and border security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00683 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.309

and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In commenting on our September 2011 report, DHS acknowledged our work to assess the progress the department has made in enhancing the nation's security and the challenges that still exist. The department discussed its views of its accomplishments since 2001, such as the creation and management of the Visa Security Program; the establishment of fusion centers to serve as focal points for the analysis and sharing on threat and vulnerability-related information; and passenger screening and prescreening programs, among other things. We recognize the department's progress in these and other areas in the report, as well as identify existing challenges that will be important for DHS to address moving forward. DHS further noted that the report did not address all of DHS's homeland security-related activities and efforts. DHS also stated that the report's assessments of progress in each homeland security mission area were not comprehensive because we and the DHS IG completed varying degrees of work for each area. We reflect in the report that it was primarily based on work we completed since DHS began operations, supplemented with the work of the DHS IG, with an emphasis on work completed since 2008 and updated information provided by DHS in July and August 2011. As such, the report identified that our work and that of the DHS IG did not cover all of DHS's homeland security-related programs and activities, and that the report was not intended to do so. Further, we noted in the report that because we and the DHS IG have completed varying degrees of work (in terms of the amount and scope of reviews completed) for each functional area, and because different DHS components and offices provided us with different amounts and types of information, the report's assessments of DHS's progress in each area reflected the information available for our review and analysis and were not necessarily equally comprehensive across all 10 areas.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00684 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.310

DHS Continues to Implement and Strengthen Its Mission Functions, but Key Operational and Management Challenges Remain

Since DHS began operations in March 2003, it has developed and implemented key policies, programs, and activities for implementing its homeland security missions and functions that have created and strengthened a foundation for achieving its potential as it continues to mature. However, the department's efforts have been hindered by challenges faced in leading and coordinating the homeland security enterprise; implementing and integrating its management functions for results; and strategically managing risk and assessing, and adjusting as necessary, its homeland security efforts.[10] DHS has made progress in these three areas, but needs to take additional action, moving forward, to help it achieve its full potential.

DHS Has Made Progress in Implementing its Mission Functions, but Program Weaknesses and Management Issues Have Hindered Implementation Efforts

DHS has made important progress in implementing and strengthening its mission functions over the past 8 years, including implementing key homeland security operations and achieving important goals and milestones in many areas. The department's accomplishments include developing strategic and operational plans across its range of missions; hiring, deploying and training workforces; establishing new, or expanding existing, offices and programs; and developing and issuing policies, procedures, and regulations to govern its homeland security operations. For example:

- DHS issued the QHSR, which provides a strategic framework for homeland security, and the National Response Framework, which outlines guiding principles for disaster response.
- DHS successfully hired, trained, and deployed workforces, such as a federal screening workforce which assumed security screening responsibilities at airports nationwide, and the department has about 20,000 agents to patrol U.S. land borders.
- DHS created new programs and offices, or expanded existing ones, to implement key homeland security responsibilities, such as establishing the United States Computer Emergency Readiness Team to, among other things, coordinate the nation's

[10] DHS defines the homeland security enterprise as the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities, who share a common national interest in the safety and security of the United States and its population.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00685 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.311

efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. DHS also expanded programs for identifying and removing aliens subject to removal from the United States and for preventing unauthorized aliens from entering the country.

- DHS issued policies and procedures addressing, among other things, the screening of passengers at airport checkpoints, inspecting travelers seeking entry into the United States, and assessing immigration benefit applications and processes for detecting possible fraud.

Establishing these elements and others are important accomplishments and have been critical for the department to position and equip itself for fulfilling its homeland security missions and functions.

However, more work remains for DHS to address gaps and weaknesses in its current operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. For example, we have reported that many DHS programs and investments have experienced cost overruns, schedule delays, and performance problems, including, for instance, DHS's recently cancelled technology program for securing U.S. borders, known as the Secure Border Initiative Network, and some technologies for screening passengers at airport checkpoints. Further, with respect to the cargo advanced automated radiography system to detect certain nuclear materials in vehicles and containers at ports DHS pursued the acquisition and deployment of the system without fully understanding that it would not fit within existing inspection lanes at ports of entry. DHS subsequently canceled the program. DHS also has not yet fully implemented its roles and responsibilities for developing and implementing key homeland security programs and initiatives. For example, DHS has not yet developed a set of target capabilities for disaster preparedness or established metrics for assessing those capabilities to provide a framework for evaluating preparedness, as required by the Post-Katrina Emergency Management Reform Act.[11] Our work has shown that DHS should take additional action to improve the efficiency and effectiveness of a number of its programs and activities by, for example, improving

[11] See 6 U.S.C. § 749.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00686 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.312

program management and oversight, and better assessing homeland security requirements, needs, costs, and benefits, such as those for key acquisition and technology programs. Table 1 provides examples of key progress and work remaining in DHS's functional mission areas, with an emphasis on work we completed since 2008.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00687 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.313

Table 1: Examples of Key Progress and Work Remaining in DHS's Efforts to Implement Its Homeland Security Missions on Which We and the DHS IG Have Reported

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 1: Preventing Terrorism and Enhancing Security	Aviation security	**Key progress:** DHS enhanced aviation security in key areas related to passenger prescreening, passenger checkpoint screening, checked baggage screening, and air cargo security. For example, DHS developed and implemented Secure Flight as a passenger prescreening program to match airline passenger information against terrorist watchlist records. DHS also deployed technology to screen passengers and checked baggage at airports. For example, in response to the December 25, 2009, attempted attack on Northwest flight 253, DHS revised the advanced imaging technology procurement and deployment strategy, increasing the planned deployment of advanced imaging technology from 878 to between 1,350 and 1,800 units.[a] Further, DHS is screening passengers using staff trained in behavior detection principles and deployed about 3,000 Behavior Detection Officers to 161 airports as part of its Screening of Passengers by Observation Techniques program. Moreover, DHS reported, as of August 2010, that it had established a system to screen 100 percent of domestic air cargo (cargo transported within and outbound from the United States) transported on passenger aircraft by, among other things, creating a voluntary program to facilitate screening throughout the air cargo supply chain and taking steps to test technologies for screening air cargo. **What remains to be done:** DHS should take additional action to strengthen its aviation security efforts. For example, a risk-based strategy and a cost-benefit analysis of airport checkpoint technologies would improve passenger checkpoint screening. TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based and did not reflect some of the key risk management principles, such as conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and did not include a cost-benefit analysis and performance measures. Further, in March 2010, we reported that it was unclear whether the advanced imaging technology would have detected the weapon used in the December 25, 2009 attempted terrorist attack based on the preliminary testing information we received. DHS also had not validated the science supporting its Screening of Passengers by Observation Techniques program, or determined if behavior detection techniques could be successfully used across the aviation system to detect threats before deploying the program. DHS completed a program validation study in April 2011 which found that the program was more effective than random screening, but that more work was needed to determine whether the science could be used for counterterrorism purposes in the aviation environment. Moreover, DHS does not yet have a plan and schedule for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements. In addition, DHS does not yet have a mechanism to verify the accuracy of domestic and inbound air cargo screening data to help ensure that screening is being conducted at reported levels, and DHS does not yet have approved technology to screen cargo once it is loaded onto a pallet or container—both of which are common means of transporting air cargo on passenger aircraft, thus requiring that screening occur before incorporation into pallets and containers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00688 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.314

QHSR mission	Functional area	Summary of key progress and work remaining
	CBRN threats	**Key progress:** DHS made progress in assessing risks posed by CBRN threats, developing CBRN detection capabilities, and planning for nuclear detection. For example, DHS develops risk assessments of CBRN threats and has issued seven classified CBRN risk assessments since 2006. DHS also assessed the threat posed by specific CBRN agents in order to determine which of those agents pose a material threat to the United States, known as material threat assessments. With regard to CBRN detection capabilities, DHS implemented the BioWatch program in more than 30 metropolitan areas to detect specific airborne biological threat agents. Further, DHS established the National Biosurveillance Integration Center to enhance the federal government's capability to identify and track biological events of national concern. In addition, DHS coordinated the development of a strategic plan for the global nuclear detection architecture—a multidepartment effort to protect against terrorist attacks using nuclear and radiological materials through coordinated activities—and has deployed radiation detection equipment. **What remains to be done:** More work remains for DHS to strengthen its CBRN assessment, detection, and mitigation capabilities. For example, DHS should better coordinate with the Department of Health and Human Services in conducting CBRN risk assessments by developing written policies and procedures governing development of the assessments. Moreover, the National Biosurveillance Integration Center lacks resources necessary for operations, such as data and personnel from its partner agencies. Additionally, work remains for DHS in its implementation of the global nuclear detection architecture. Specifically, the strategic plan for the architecture did not include some key components, such as funding needed to achieve the strategic plan's objectives, or monitoring mechanisms for determining programmatic progress and identifying needed improvements. DHS officials told us that they will address these missing elements in an implementation plan, which they plan to issue by the end of 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00689 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.315

QHSR mission	Functional area	Summary of key progress and work remaining
	Critical infrastructure protection – physical assets	**Key progress:** DHS expanded its efforts to conduct risk assessment and planning, provide for protection and resiliency, and implement partnerships and coordination mechanisms for physical critical assets. For example, DHS updated the National Infrastructure Protection Plan to include an emphasis on resiliency (the capacity to resist, absorb, or successfully adapt, respond to, or recover from disasters), and enhanced discussion about DHS risk management. Moreover, DHS components with responsibility for critical infrastructure sectors, such as transportation security, have begun to use risk-based assessments in their critical infrastructure related planning and protection efforts. Further, DHS has various voluntary programs in place to conduct vulnerability assessments and security surveys at and across facilities from the 18 critical infrastructure sectors, and uses these assessments to develop and disseminate information on steps asset owners and operators can take to protect their facilities. In addition, DHS coordinated with critical infrastructure stakeholders, including other federal regulatory authorities to identify overlaps and gaps in critical infrastructure security activities. **What remains to be done:** Additional actions are needed for DHS to strengthen its critical infrastructure protection programs and efforts. For example, DHS has not fully implemented an approach to measure its effectiveness in working with critical asset owners and operators in their efforts to adopt measures to mitigate resiliency gaps identified during various vulnerability assessments. Moreover, DHS components have faced difficulties in incorporating risk-based assessments in critical infrastructure planning and protection efforts, such as in planning for security in surface transportation modes like highway infrastructure. Further, DHS should determine the feasibility of developing an approach to disseminating information on resiliency practices to its critical infrastructure partners to better position itself to help asset owners and operators consider and adopt resiliency strategies, and provide them with information on potential security investments.
	Surface transportation security	**Key progress:** DHS expanded its efforts in key surface transportation security areas, such as risk assessments and strategic planning; the surface transportation inspector workforce; and information sharing. For example, DHS conducted risk assessments of surface transportation modes and developed a transportation sector security risk assessment that assessed risk within and across the various modes. Further, DHS more than doubled its surface transportation inspector workforce and, as of July 2011, reported that its surface inspectors had conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, among other things. Moreover, DHS allocates transit grant funding based on risk assessments and has taken steps to measure performance of its Transit Security Grant Program, which provides funds to owners and operators of mass transit and passenger rail systems. In addition, DHS expanded its sharing of surface transportation security information by establishing information networks. **What remains to be done:** DHS should take further action to strengthen its surface transportation security programs and operations. For example, DHS's efforts to improve elements of risk assessments of surface transportation modes are in the early stages of implementation. Moreover, DHS noted limitations in its transportation sector security risk assessment—such as the exclusion of threats from "lone wolf" operators—that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. Further, DHS has not yet completed a long-term workforce plan that identifies future needs for its surface transportation inspector workforce. It also has not yet issued regulations for a training program for mass transit, rail, and bus employees, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[b] Additionally, DHS's information sharing efforts would benefit from improved streamlining, coordination, and assessment of the effectiveness of information sharing mechanisms.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00690 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.316

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 2: Securing and Managing Our Borders	Border security	**Key progress:** DHS expanded its efforts in key border security areas, such as inspection of travelers and cargo at ports of entry, security of the border between ports of entry, visa adjudication security, and collaboration with stakeholders. Specifically, DHS has undertaken efforts to keep terrorists and other dangerous people from entering the country. For example, DHS implemented the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information. DHS established plans for, and had begun to interact with and involve stakeholders in, developing an exit capability. DHS deployed technologies and other infrastructure to secure the border between ports of entry, including more than 600 miles of tactical infrastructure, such as fencing, along the border. DHS also deployed the Visa Security Program, in which DHS personnel review visa applications to help prevent individuals who pose a threat from entering the United States, to 19 posts in 15 countries, and developed a 5-year expansion plan for the program. In addition, DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts through, among other things, the establishment of interagency forums. **What remains to be done:** More work remains for DHS to strengthen its border security programs and operations. For example, although it has developed a plan, DHS has not yet adopted an integrated approach to scheduling, executing, and tracking the work needed to be accomplished to deliver a comprehensive biometric exit solution as part of the US-VISIT program. Further, DHS experienced schedule delays and performance problems with its information technology program for securing the border between ports of entry—the Secure Border Initiative Network—which led to its cancellation. Because of the program's decreased scope, uncertain timing, unclear costs, and limited life cycle management, it was unclear whether DHS's pursuit of the program was cost-effective. DHS is transitioning to a new approach for border technology, which we are assessing. With regard to the Visa Security Program, DHS did not fully follow or update its 5-year expansion plan. For instance, it did not establish 9 posts identified for expansion in 2009 and 2010, and had not taken steps to address visa risk at posts that did not have a Visa Security Program presence. Additionally, DHS should strengthen its oversight of interagency forums operating along the northern border.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00691 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.317

QHSR mission	Functional area	Summary of key progress and work remaining
	Maritime security	**Key progress:** DHS expanded its efforts in key maritime security areas, such as port facility and vessel security, maritime security domain awareness and information sharing, and international supply chain security. For example, DHS strengthened risk management through the development of a risk assessment model, and addressed risks to port facilities through annual inspections in which DHS identified and corrected deficiencies, such as facilities failing to follow security plans for access control. Further, DHS took action to address risks posed by foreign seafarers entering U.S. seaports by, for example, conducting advance-screening before the arrival of vessels at U.S. ports, inspections, and enforcement operations. DHS developed the Transportation Worker Identification Credential program to manage the access of unescorted maritime workers to secure areas of regulated maritime facilities. DHS also implemented measures to help secure passenger vessels including cruise ships, ferries, and energy commodity vessels such as tankers, such as assessing risks to these types of vessels. Moreover, for tracking vessels at sea, the Coast Guard uses a long-range identification and tracking system, and a commercially provided long-range automatic identification system. For tracking vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system, and also either operates, or has access to, radar and cameras in some ports. DHS also developed a layered security strategy for cargo container security, including deploying screening technologies and partnering with foreign governments. **What remains to be done:** DHS should take additional action to strengthen its maritime security efforts. For example, because of a lack of technology capability, DHS did not electronically verify identity and immigration status of foreign seafarers, as part of its onboard admissibility inspections of cargo vessels, thus limiting the assurance that fraud could be identified among documents presented by them. In addition, the Transportation Worker Identification Credential program's controls were not designed to provide reasonable assurance that only qualified applicants acquire credentials. For example, during covert tests of the Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Moreover, DHS has not assessed the costs and benefits of requiring cruise lines to provide passenger reservation data for screening, which could help improve identification and targeting of potential terrorists. Further, the vessel tracking systems used in U.S. coastal areas, inland waterways, and ports had more difficulty tracking smaller and noncommercial vessels because these vessels were not generally required to carry automatic identification system equipment, and because of the technical limitations of radar and cameras. In addition, DHS has made limited progress in scanning containers at the initial ports participating in the Secure Freight Initiative, a program at selected ports with the intent of scanning 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas, leaving the feasibility of 100 percent scanning largely unproven. CBP has not yet developed a plan for full implementation of a statutory requirement that 100 percent of U.S.-bound container cargo be scanned by 2012.[c]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00692 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.318

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 3: Enforcing and Administering Our Immigration Laws	Immigration enforcement	**Key progress:** DHS expanded its immigration and customs enforcement programs and activities in key areas such as overstay enforcement, compliance with workplace immigration laws, alien smuggling, and firearms trafficking. For example, DHS increased its resources for investigating overstays (unauthorized immigrants who entered the United States legally on a temporary basis then overstayed their authorized periods of admission) and alien smuggling operations, and deployed border enforcement task forces to investigate illicit smuggling of people and goods, including firearms. In addition, DHS took action to improve the E-Verify program, which provides employers a voluntary tool for verifying an employee's authorization to work in the United States, by, for example, increasing the program's accuracy by expanding the number of databases it can query. Further, DHS expanded its programs and activities to identify and remove criminal aliens in federal, state, and local custody who are eligible for removal from the United States by, for example, entering into agreements with state and local law enforcement agencies to train officers to assist in identifying those individuals who are in the United States illegally. **What remains to be done:** Key weaknesses remain in DHS's immigration and customs enforcement efforts. For example, DHS took action to address a small portion of the estimated overstay population in the United States, and lacks measures for assessing its progress in addressing overstays. In particular, DHS field offices had closed about 34,700 overstay investigations assigned to them from fiscal year 2004 through 2010, as of October 2010; these cases resulted in approximately 8,100 arrests, relative to a total estimated overstay population of 4 million to 5.5 million.[d] Additionally, we reported that since fiscal year 2006, U.S. Immigration and Customs Enforcement within DHS allocated about 3 percent of its investigative work hours to overstay investigations Moreover, DHS should better leverage opportunities to strengthen its alien smuggling enforcement efforts by assessing the possible use of various investigative techniques, such as those to follow cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. Further, weaknesses with the E-Verify program, including challenges in accurately estimating E-Verify costs, put DHS at an increased risk of not making informed investment decisions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00693 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.319

QHSR mission	Functional area	Summary of key progress and work remaining
	Immigration services	**Key progress:** DHS improved the quality and efficiency of the immigration benefit administration process, and expanded its efforts to detect and deter immigration fraud. For example, DHS initiated efforts to modernize its immigration benefit administration infrastructure; improve the efficiency and timeliness of its application intake process; and ensure quality in its benefit adjudication processes. Further, DHS designed training programs and quality reviews to help ensure the integrity of asylum adjudications. Moreover, in 2004 DHS established the Office of Fraud Detection and National Security, now a directorate, to lead immigration fraud detection and deterrence efforts, and this directorate has since developed and implemented strategies for this purpose. **What remains to be done:** More work remains in DHS's efforts to improve its administration of immigration benefits. For example, DHS's program for transforming its immigration benefit processing infrastructure and business practices from paper-based to digital systems missed its planned milestones by more than 2 years, and has been hampered by management challenges, such as insufficient planning and not adhering to DHS acquisition guidance before selecting a contractor to assist with implementation of the transformation program. Additionally, while the Fraud Detection and National Security Directorate put in place strategies for detecting and deterring immigration fraud, DHS should take additional action to address vulnerabilities identified in its assessments intended to determine the extent and nature of fraud in certain applications. Further, despite mechanisms DHS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers we surveyed cited challenges in identifying fraud as a key factor affecting their adjudications. For example, 73 percent of asylum officer survey respondents reported it was moderately or very difficult to identify document fraud.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00694 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.320

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 4: Safeguarding and Securing Cyberspace	Critical infrastructure protection – cyber assets	**Key progress:** DHS expanded its efforts to conduct cyber security risk assessments and planning, provide for the protection and resilience of cyber assets, and implement cyber security partnerships and coordination mechanisms. For example, DHS developed the first National Cyber Incident Response Plan in September 2010 to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels. DHS also took steps to secure external network connections in use by the federal government by establishing the National Cybersecurity Protection System, operationally known as Einstein, to analyze computer network traffic information to and from agencies. In 2008, DHS developed Einstein 2, which incorporated network intrusion detection technology into the capabilities of the initial version of the system. Additionally, the department made progress in enhancing its cyber analysis and incident warning capabilities through the establishment of the U.S. Computer Emergency Readiness Team, which, among other things, coordinates the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. Moreover, since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing lessons it had learned from this exercise to strengthen public and private incident response capabilities. **What remains to be done:** Key challenges remain in DHS's cyber security efforts. For example, to expand its protection and resiliency efforts, DHS needs to lead a concerted effort to consolidate and better secure Internet connections at federal agencies. Further, DHS faced challenges regarding deploying Einstein 2, including understanding the extent to which its objective was being met because the department lacked performance measures that addressed whether agencies report whether the alerts represent actual incidents. DHS also faces challenges in fully establishing a comprehensive national cyber analysis and warning capability. For example, the U.S. Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities. These attributes are related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, the U.S. Computer Emergency Readiness Team provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. Additionally, expectations of private sector stakeholders are not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00695 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.321

QHSR mission	Functional area	Summary of key progress and work remaining
Mission 5: Ensuring Resilience to Disasters	Emergency preparedness and response	**Key progress:** DHS expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; and enhanced emergency communications. For example, DHS developed various plans for disaster preparedness and response. In particular, in 2004 DHS issued the National Response Plan and subsequently made revisions to it, culminating in the issuance of the National Response Framework in January 2008, which outlines the guiding principles and major roles and responsibilities of government, nongovernmental organizations, and private sector entities for response to disasters of all sizes and causes. Further, DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-based preparedness, and a Target Capabilities List, designed to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS also assisted local communities with developing long-term disaster recovery plans as part of its post-disaster assistance. For example, DHS assisted Iowa City's recovery from major floods in 2008 by, among other things, identifying possible federal funding sources for specific projects in the city's recovery plan, and advising the city on how to prepare effective project proposals. DHS is also finalizing a National Disaster Recovery Framework, intended to provide a model to identify and address challenges that arise during the disaster recovery process. Moreover, DHS issued the National Emergency Communications Plan—the first strategic document for improving emergency communications nationwide. **What remains to be done:** More work remains in DHS's efforts to assess capabilities to define all-hazards and provide long-term disaster recovery assistance. For example, DHS has not yet developed national preparedness capability requirements based on established metrics to provide a framework for assessing preparedness. Further, the data DHS collected to measure national preparedness were limited by reliability and measurement issues related to the lack of standardization. Until a framework for assessing preparedness is in place, DHS will not have a basis on which to operationalize and implement its conceptual approach for assessing local, state, and federal preparedness capabilities against capability requirements and identify capability gaps for prioritizing investments in national preparedness. Moreover, with regard to long-term disaster recovery assistance, DHS's criteria for when to provide the assistance were vague, and, in some cases, DHS provided assistance before state and local governments had the capacity to work effectively with DHS. Additionally, DHS should improve the efficacy of the grant application and review process by mitigating duplication or redundancy within the various preparedness grant programs. Until DHS evaluates grant applications across grant programs, DHS cannot ascertain whether or to what extent multiple funding requests are being submitted for similar purposes.

Source: GAO analysis based on the areas included in our September 2011 report.

[a] Advanced imaging technology units produce an image of a passenger's body that DHS personnel use to look for anomalies, such as explosives or other prohibited items.

[b] The Implementing Recommendations of the 9/11 Commission Act requires TSA to issue regulations for a training program to prepare mass transit, rail, and over-the-road bus employees for potential security threats and conditions. 6 U.S.C. §§ 1137, 1167, 1184.

[c] See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-490 (2007) (amending 6 U.S.C. § 982(b)).

[d] According to our April 2011 report, the most recent estimates from the Pew Hispanic Center approximated that, in 2006, out of an unauthorized resident alien population of 11.5 million to 12 million in the United States, about 4 million to 5.5 million were overstays. Pew Hispanic Center, *Modes of Entry for the Unauthorized Migrant Population* (Washington, D.C.: May 22, 2006).

Impacting the department's ability to efficiently and effectively satisfy its missions are: (1) the need to integrate and strengthen its management

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00696 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.322

functions; (2) the need for increased utilization of performance assessments; (3) the need for an enhanced use of risk information to inform planning, programming, and investment decision-making; (4) limitations in effective sharing and use of terrorism-related information; (5) partnerships that are not sustained or fully leveraged; and (6) limitations in developing and deploying technologies to meet mission needs. DHS made progress in addressing these areas, but more work is needed, going forward, to further mitigate these challenges and their impact on DHS's mission implementation.

For instance, DHS strengthened its performance measures in recent years and linked its measures to the QHSR's missions and goals. However, DHS and its components have not yet developed measures for assessing the effectiveness of key homeland security programs, such as programs for securing the border and preparing the nation for emergency incidents. For example, with regard to checkpoints DHS operates on U.S. roads to screen vehicles for unauthorized aliens and contraband, DHS established three performance measures to report the results of checkpoint operations. However, the measures did not indicate if checkpoints were operating efficiently and effectively and data reporting and collection challenges hindered the use of results to inform Congress and the public on checkpoint performance. Moreover, DHS has not yet established performance measures to assess the effectiveness of its programs for investigating alien smuggling operations and foreign nationals who overstay their authorized periods of admission to the United States, making it difficult for these agencies to determine progress made in these areas and evaluate possible improvements.

Further, DHS and its component agencies developed strategies and tools for conducting risk assessments. For example, DHS has conducted risk assessments of various surface transportation modes, such as freight rail, passenger rail, and pipelines. However, the department needs to strengthen its use of risk information to inform its planning and investment decision-making. For example, DHS could better use risk information to plan and prioritize security measures and investments within and across its mission areas, as the department cannot secure the nation against every conceivable threat.

In addition, DHS took action to develop and deploy new technologies to help meet its homeland security missions. However, in a number of instances DHS pursued acquisitions without ensuring that the technologies met defined requirements, conducting and documenting appropriate testing and evaluation, and performing cost-benefit analyses,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00697 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.323

resulting in important technology programs not meeting performance expectations. For example, in 2006, we recommended that DHS's decision to deploy next-generation radiation-detection equipment, or advanced spectroscopic portals, used to detect smuggled nuclear or radiological materials, be based on an analysis of both the benefits and costs and a determination of whether any additional detection capability provided by the portals was worth their additional cost. DHS subsequently issued a cost-benefit analysis, but we reported that this analysis did not provide a sound analytical basis for DHS's decision to deploy the portals. In June 2009, we also reported that an updated cost-benefit analysis might show that DHS's plan to replace existing equipment with advanced spectroscopic portals was not justified, particularly given the marginal improvement in detection of certain nuclear materials required of advanced spectroscopic portals and the potential to improve the current-generation portal monitors' sensitivity to nuclear materials, most likely at a lower cost. In July 2011, DHS announced that it would end the advanced spectroscopic portal project as originally conceived given the challenges the program faced.

As we have previously reported, while it is important that DHS continue to work to strengthen each of its functional areas, it is equally important that these areas be addressed from a comprehensive, departmentwide perspective to help mitigate longstanding issues that have impacted the department's progress.

Key Themes Have Impacted DHS's Progress in Implementing Its Mission Functions

Our work at DHS has identified several key themes—leading and coordinating the homeland security enterprise, implementing and integrating management functions for results, and strategically managing risks and assessing homeland security efforts—that have impacted the department's progress since it began operations. These themes provide insights that can inform DHS's efforts, moving forward, as it works to implement its missions within a dynamic and evolving homeland security environment. DHS made progress and has had successes in all of these areas, but our work found that these themes have been at the foundation of DHS's implementation challenges, and need to be addressed from a departmentwide perspective to position DHS for the future and enable it to satisfy the expectations set for it by the Congress, the administration, and the country.

Leading and coordinating the homeland security enterprise. While DHS is one of a number of entities with a role in securing the homeland, it has significant leadership and coordination responsibilities for managing

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00698 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.324

efforts across the homeland security enterprise. To satisfy these responsibilities, it is critically important that DHS develop, maintain and leverage effective partnerships with its stakeholders, while at the same time addressing DHS-specific responsibilities in satisfying its missions. Before DHS began operations, we reported that the quality and continuity of the new department's leadership would be critical to building and sustaining the long-term effectiveness of DHS and achieving homeland security goals and objectives. We further reported that to secure the nation, DHS must form effective and sustained partnerships between components and also with a range of other entities, including federal agencies, state and local governments, the private and nonprofit sectors, and international partners.

DHS has made important strides in providing leadership and coordinating efforts. For example, it has improved coordination and clarified roles with state and local governments for emergency management. DHS also strengthened its partnerships and collaboration with foreign governments to coordinate and standardize security practices for aviation security. However, DHS needs to take additional action to forge effective partnerships and strengthen the sharing and utilization of information, which has affected its ability to effectively satisfy its missions. For example, we reported that the expectations of private sector stakeholders have not been met by DHS and its federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. Without improvements in meeting private and public sector expectations for sharing cyber threat information, private-public partnerships will remain less than optimal, and there is a risk that owners of critical infrastructure will not have the information and mechanisms needed to thwart sophisticated cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure. Moreover, we reported that DHS needs to continue to streamline its mechanisms for sharing information with public transit agencies to reduce the volume of similar information these agencies receive from DHS, making it easier for them to discern relevant information and take appropriate actions to enhance security.

In 2005, we designated information sharing for homeland security as high risk because the federal government faced serious challenges in analyzing information and sharing it among partners in a timely, accurate, and useful way. Gaps in sharing, such as agencies' failure to link information about the individual who attempted to conduct the December 25, 2009, airline bombing, prevented the individual from being included on the federal government's consolidated terrorist watchlist, a tool used

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00699 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.325

by DHS to screen for persons who pose a security risk. The federal government and DHS have made progress, but more work remains for DHS to streamline its information sharing mechanisms and better meet partners' needs. Moving forward, it will be important that DHS continue to enhance its focus and efforts to strengthen and leverage the broader homeland security enterprise, and build off the important progress that it has made thus far. In addressing ever-changing and complex threats, and with the vast array of partners with which DHS must coordinate, continued leadership and stewardship will be critical in achieving this end.

Implementing and integrating management functions for results. Following its establishment, the department focused its efforts primarily on implementing its various missions to meet pressing homeland security needs and threats, and less on creating and integrating a fully and effectively functioning department from 22 disparate agencies. This initial focus on mission implementation was understandable given the critical homeland security needs facing the nation after the department's establishment, and the enormous challenge posed by creating, integrating, and transforming a department as large and complex as DHS. As the department matured, it has put into place management policies and processes and made a range of other enhancements to its management functions—acquisition, information technology, financial, and human capital management. However, DHS has not always effectively executed or integrated these functions. In 2003, we designated the transformation and integration of DHS as high risk because DHS had to transform 22 agencies into one department, and failure to effectively address DHS's management and mission risks could have serious consequences for U.S. national and economic security. Eight years later, DHS remains on our high-risk list. DHS has demonstrated strong leadership commitment to addressing its management challenges and has begun to implement a strategy to do so. Further, DHS developed various management policies, directives, and governance structures, such as acquisition and information technology management policies and controls, to provide enhanced guidance on investment decision making. DHS also reduced its financial management material weaknesses in internal control over financial reporting and developed strategies to strengthen human capital management, such as its *Workforce Strategy for Fiscal Years 2011-2016*.

However, DHS needs to continue to demonstrate sustainable progress in addressing its challenges, as these issues have contributed to schedule delays, cost increases, and performance problems in major programs aimed at delivering important mission capabilities. For example, in

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00700 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.326

September 2010, we reported that the Science and Technology Directorate's master plans for conducting operational testing of container security technologies did not reflect all of the operational scenarios that U.S. Customs and Border Protection was considering for implementation. In addition, when it developed the US-VISIT program, DHS did not sufficiently define what capabilities and benefits would be delivered, by when, and at what cost, and the department has not yet determined how to deploy a biometric exit capability under the program. Moreover, DHS does not yet have enough skilled personnel to carry out activities in various areas, such as acquisition management; and has not yet implemented an integrated financial management system, impacting its ability to have ready access to reliable, useful, and timely information for informed decision making. Moving forward, addressing these management challenges will be critical for DHS's success, as will be the integration of these functions across the department to achieve efficiencies and effectiveness.

Strategically managing risks and assessing homeland security efforts. Forming a new department while working to implement statutorily mandated and department-initiated programs and responding to evolving threats, was, and is, a significant challenge facing DHS. Key threats, such as attempted attacks against the aviation sector, have impacted and altered DHS's approaches and investments, such as changes DHS made to its processes and technology investments for screening passengers and baggage at airports. It is understandable that these threats had to be addressed immediately as they arose. However, limited strategic and program planning by DHS and limited assessment to inform approaches and investment decisions have contributed to programs not meeting strategic needs or not doing so in an efficient manner. For example, as we reported in July 2011, the Coast Guard's planned acquisitions through its Deepwater Program, which began before DHS's creation and includes efforts to build or modernize ships and aircraft and supporting capabilities that are critical to meeting the Coast Guard's core missions in the future, is unachievable due to cost growth, schedule delays and affordability issues. In addition, because FEMA has not yet developed a set of target disaster preparedness capabilities and a systematic means of assessing those capabilities, as required by the Post-Katrina Emergency Management Reform Act and Presidential Policy Directive 8, it cannot effectively evaluate and identify key capability gaps and target limited resources to fill those gaps.

Further, DHS has made important progress in analyzing risk across sectors, but it has more work to do in using this information to inform

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00701 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.327

planning and resource allocation decisions. Risk management has been widely supported by Congress and DHS as a management approach for homeland security, enhancing the department's ability to make informed decisions and prioritize resource investments. Since DHS does not have unlimited resources and cannot protect the nation from every conceivable threat, it must make risk-informed decisions regarding its homeland security approaches and strategies.

Moreover, we have reported on the need for enhanced performance assessment, that is, evaluating existing programs and operations to determine whether they are operating as intended or are in need of change, across DHS's missions. Information on the performance of programs is critical for helping the department, Congress, and other stakeholders more systematically assess strengths and weaknesses and inform decision making. In recent years, DHS has placed an increased emphasis on strengthening its mechanisms for assessing the performance and effectiveness of its homeland security programs. For example, DHS established new performance measures, and modified existing ones, to better assess many of its programs and efforts.

However, our work has found that DHS continues to miss opportunities to optimize performance across its missions because of a lack of reliable performance information or assessment of existing information; evaluation among feasible alternatives; and, as appropriate, adjustment of programs or operations that are not meeting mission needs. For example, DHS's program for research, development, and deployment of passenger checkpoint screening technologies lacked a risk-based plan and performance measures to assess the extent to which checkpoint screening technologies were achieving the program's security goals, and thereby reducing or mitigating the risk of terrorist attacks. As a result, DHS had limited assurance that its strategy targeted the most critical risks and that it was investing in the most cost-effective new technologies or other protective measures. As the department further matures and seeks to optimize its operations, DHS will need to look beyond immediate requirements; assess programs' sustainability across the long term, particularly in light of constrained budgets; and evaluate tradeoffs within and among programs across the homeland security enterprise. Doing so should better equip DHS to adapt and respond to new threats in a sustainable manner as it works to address existing ones.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00702 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.328

Concluding Observations

Given DHS's role and leadership responsibilities in securing the homeland, it is critical that the department's programs and activities are operating as efficiently and effectively as possible, are sustainable, and continue to mature, evolve and adapt to address pressing security needs. DHS has made significant progress throughout its missions since its creation, but more work is needed to further transform the department into a more integrated and effective organization. DHS has also made important progress in strengthening partnerships with stakeholders, improving its management processes and sharing of information, and enhancing its risk management and performance measurement efforts. These accomplishments are especially noteworthy given that the department has had to work to transform itself into a fully functioning cabinet department while implementing its missions—a difficult undertaking for any organization and one that can take years to achieve even under less daunting circumstances.

Impacting the department's efforts have been a variety of factors and events, such as attempted terrorist attacks and natural disasters, as well as new responsibilities and authorities provided by Congress and the administration. These events collectively have forced DHS to continually reassess its priorities and reallocate resources as needed, and have impacted its continued integration and transformation. Given the nature of DHS's mission, the need to remain nimble and adaptable to respond to evolving threats, as well as to work to anticipate new ones, will not change and may become even more complex and challenging as domestic and world events unfold, particularly in light of reduced budgets and constrained resources. To better position itself to address these challenges, our work has shown that DHS should place an increased emphasis and take additional action in supporting and leveraging the homeland security enterprise, managing its operations to achieve needed results, and strategically planning for the future while assessing and adjusting, as needed, what exists today. Addressing these issues will be critically important for the department to strengthen its homeland security programs and operations. Eight years after its establishment and 10 years after the September 11, 2001, terrorist attacks, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, this concludes my prepared statement. I would be pleased to respond to any questions you may have at this time.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00703 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.329

Contacts and Acknowledgments

For further information regarding this testimony, please contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Rebecca Gambler, Assistant Director; Melissa Bogar; Susan Czachor; Sarah Kaczmarek; Tracey King; Taylor Matheson; Jessica Orr; and Meghan Squires.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00704 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.330

United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2011

DEPARTMENT OF HOMELAND SECURITY

Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

U.S. Government Accountability Office

GAO 90 YEARS 1921-2011

ACCOUNTABILITY * INTEGRITY * RELIABILITY

GAO-11-881

67123.331

September 2011

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-11-881, a report to congressional requesters

DEPARTMENT OF HOMELAND SECURITY

Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11

Why GAO Did This Study

The events of September 11, 2001, led to profound changes in government policies and structures to confront homeland security threats. Most notably, the Department of Homeland Security (DHS) began operations in 2003 with key missions that included preventing terrorist attacks from occurring in the United States, and minimizing the damages from any attacks that may occur. DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. Since 2003, GAO has issued over 1,000 products on DHS's operations in such areas as border and transportation security and emergency management, among others. As requested, this report addresses DHS's progress in implementing its homeland security missions since it began operations, work remaining, and issues affecting implementation efforts. This report is based on GAO's past and ongoing work, supplemented with DHS Office of Inspector General reports, with an emphasis on reports issued since 2008. GAO also analyzed information provided by DHS in July and August 2011 on recent actions taken in response to prior work.

What GAO Recommends

While this report contains no new recommendations, GAO previously made about 1,500 recommendations to DHS. The department addressed about half of them, has efforts under way to address others, and has taken additional action to strengthen its operations. In commenting on this report, DHS stated that the report did not address all of DHS's activities. This report is based on prior work, which GAO reflects throughout the report.

View GAO-11-881 or key components.
For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

Since it began operations in 2003, DHS has implemented key homeland security operations and achieved important goals and milestones in many areas to create and strengthen a foundation to reach its potential. As it continues to mature, however, more work remains for DHS to address gaps and weaknesses in its current operational and implementation efforts, and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. DHS's accomplishments include developing strategic and operational plans; deploying workforces; and establishing new, or expanding existing, offices and programs. For example, DHS

- issued plans to guide its efforts, such as the Quadrennial Homeland Security Review, which provides a framework for homeland security, and the *National Response Framework*, which outlines disaster response guiding principles;
- successfully hired, trained, and deployed workforces, such as a federal screening workforce to assume security screening responsibilities at airports nationwide; and
- created new programs and offices to implement its homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to help coordinate efforts to address cybersecurity threats.

Such accomplishments are noteworthy given that DHS has had to work to transform itself into a fully functioning department while implementing its missions—a difficult undertaking that can take years to achieve. While DHS has made progress, its transformation remains high risk due to its management challenges. Examples of progress made and work remaining include:

Border security. DHS implemented the U.S. Visitor and Immigrant Status Indicator Technology program to verify the identities of foreign visitors entering and exiting the country by processing biometric and biographic information. However, DHS has not yet determined how to implement a biometric exit capability and has taken action to address a small portion of the estimated overstay population in the United States (individuals who legally entered the country but then overstayed their authorized periods of admission). DHS also deployed infrastructure to secure the border between ports of entry, including more than 600 miles of fencing. However, DHS experienced schedule delays and performance problems with the Secure Border Initiative Network, which led to the cancellation of this information technology program.

Aviation security. DHS developed and implemented Secure Flight, a program for screening airline passengers against terrorist watchlist records. DHS also developed new programs and technologies to screen passengers, checked baggage, and air cargo. However, DHS does not yet have a plan for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements, a mechanism to verify the accuracy of data to help ensure that air cargo screening is being conducted at reported levels, or approved technology to screen cargo once it is loaded onto a pallet or container.

Emergency preparedness and response. DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00706 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.332

based preparedness, and a Target Capabilities List to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS is also finalizing a National Disaster Recovery Framework, and awards preparedness grants based on a reasonable risk methodology. However, DHS needs to strengthen its efforts to assess capabilities for all-hazards preparedness, and develop a long-term recovery structure to better align timing and involvement with state and local governments' capacity. DHS should also improve the efficacy of the grant application process by mitigating duplication or redundancy within the various preparedness grant programs.

Chemical, biological, radiological and nuclear (CBRN) threats. DHS assessed risks posed by CBRN threats and deployed capabilities to detect CBRN threats. However, DHS should work to improve its coordination of CBRN risk assessments, and identify monitoring mechanisms for determining progress made in implementing the global nuclear detection strategy.

GAO's work identified three themes at the foundation of DHS's challenges.

Leading and coordinating the homeland security enterprise. DHS has made important strides in providing leadership and coordinating efforts among its stakeholders. However, DHS needs to take additional action to forge effective partnerships and strengthen the sharing and utilization of information, which has affected its ability to effectively satisfy its missions. For example, the expectations of private sector stakeholders have not been met by DHS and its federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. In 2005, GAO designated information sharing for homeland security as high risk because the federal government faced challenges in analyzing and sharing information in a timely, accurate, and useful way.

Implementing and integrating management functions for results. DHS has enhanced its management functions, and has plans in place to further strengthen the management of the department for results. However, DHS has not always effectively executed or integrated these functions. In 2003, GAO designated the transformation of DHS as high risk because DHS had to transform 22 agencies into one department. DHS has demonstrated strong leadership commitment and begun to implement a strategy to address its management challenges. However, these challenges have contributed to schedule delays, cost increases, and performance problems in a number of programs aimed at delivering important mission capabilities, such as a system to detect certain nuclear materials in vehicles and containers at ports. DHS also faced difficulties in deploying some technologies that meet defined requirements. Further, DHS does not yet have enough skilled personnel in various areas, such as acquisition management; and has not yet developed an integrated financial management system, impacting its ability to have ready access to reliable information for informed decision making.

Strategically managing risks and assessing homeland security efforts. Forming a new department while working to implement statutorily mandated and department-initiated programs and responding to evolving threats, was, and is, a significant challenge facing DHS. Key threats have impacted DHS's approaches and investments. It is understandable that these threats had to be addressed immediately as they arose. However, limited strategic and program planning by DHS and limited assessment to inform approaches and investment decisions have contributed to programs not meeting strategic needs in an efficient manner.

Given DHS's leadership responsibilities in homeland security, it is critical that its programs are operating as efficiently and effectively as possible, are sustainable, and continue to mature to address pressing security needs. Eight years after its creation and 10 years after September 11, 2001, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00707 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.333

Contents

Letter		1
	Background	10
	DHS Continues to Implement and Strengthen Its Mission Functions, but Key Operational and Management Challenges Remain	16
	Agency Comments and Our Evaluation	37
Appendix I	Department of Homeland Security Functional Mission Areas, Sub-Areas, and Performance Expectations	40
Appendix II	Scope and Methodology	47
Appendix III	Aviation Security	55
Appendix IV	Chemical, Biological, Radiological, and Nuclear Threats	66
Appendix V	Critical Infrastructure Protection—Physical Assets	72
Appendix VI	Surface Transportation Security	81
Appendix VII	Border Security	91
Appendix VIII	Maritime Security	103

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00708 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.334

Appendix IX	Immigration Enforcement	116
Appendix X	Immigration Services	123
Appendix XI	Critical Infrastructure Protection—Cyber Assets	130
Appendix XII	Emergency Preparedness and Response	140
Appendix XIII	Department of Homeland Security Transformation and Implementation	152
Appendix XIV	Performance Measurement	162
Appendix XV	Risk Management	167
Appendix XVI	Information Sharing	175
Appendix XVII	Partnerships and Coordination	181
Appendix XVIII	Developing and Deploying New Technologies for Homeland Security	186

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00709 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.335

Appendix XIX	Comments from the Department of Homeland Security	192
Appendix XX	GAO Contact and Staff Acknowledgments	197
Related Reports		198

Tables

Table 1: DHS Budget Authority for Fiscal Years 2004 through 2011 in Thousands of Dollars, as Reported by DHS 12
Table 2: Examples of Key Progress and Work Remaining in DHS's Efforts to Implement Its Homeland Security Missions on Which We Have Reported 199
Table 3: Crosscutting and Management Issues Affecting DHS's Progress in Implementing Its Homeland Security Missions 29
Table 4: DHS Functional Areas, Sub-Areas, and Performance Expectations 40
Table 5: Example of Performance Expectations and Sub-Areas for Border Security 49
Table 6: Alignment of Functional Areas under DHS's QHSR Missions 51
Table 7: Assessment of Progress and Work Remaining in Key Aviation Security Areas on Which We Have Reported 57
Table 8: Assessment of Progress and Work Remaining in Key CBRN Threats Areas on Which We Have Reported 68
Table 9: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection–Physical Assets Areas on Which We Have Reported 74
Table 10: Assessment of Progress and Work Remaining in Key Surface Transportation Security Areas on Which We Have Reported 83
Table 11: Assessment of Progress and Work Remaining in Key Border Security Areas on Which We Have Reported 93
Table 12: Assessment of Progress and Work Remaining in Key Maritime Security Areas on Which We Have Reported 106
Table 13: Assessment of Progress and Work Remaining in Key Immigration Enforcement Areas on Which We Have Reported 118

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00710 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.336

Table 14: Assessment of Progress and Work Remaining in Key Immigration Services Areas on Which We Have Reported 125
Table 15: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection—Cyber Assets Areas on Which We Have Reported 133
Table 16: Assessment of Progress and Work Remaining in Emergency Preparedness and Response on Which We Have Reported 142

Figures

Figure 1: Selected Events That Have Affected DHS Implementation Efforts 15
Figure 2: GAO Risk Management Framework 168
Figure 3: DHS Risk Management Framework 170

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00711 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.337

Abbreviations

ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BUR	Bottom-Up Review
CBP	U.S. Customs and Border Protection
CBRN	chemical, biological, radiological, and nuclear
CS&C	Office of Cyber Security and Communications
CTCEU	Counterterrorism and Criminal Exploitation Unit
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
ICE	U.S. Immigration and Customs Enforcement
IG	Inspector General
NPPD	National Protection and Programs Directorate
QHSR	Quadrennial Homeland Security Review
S&T	Science and Technology Directorate
SBI	Secure Border Initiative
SBI*net*	Secure Border Initiative Network
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00712 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.338

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

September 7, 2011

The Honorable Joseph Lieberman
Chairman
The Honorable Susan Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The nation is about to pass the 10-year anniversary of the September 11, 2001, terrorist attacks. The events of that day led to profound changes in government agendas, policies, and structures to confront homeland security threats facing the nation. Most notably, in the aftermath of the attacks, the Department of Homeland Security (DHS) was created with key missions that include preventing terrorist attacks from occurring within the United States, reducing U.S. vulnerability to terrorism, minimizing resulting damages, and helping the nation recover from any attacks that may occur. The 10-year anniversary of 9/11 provides an opportunity to reflect on the progress DHS has made since its establishment and challenges it has faced in implementing its missions, as well as to identify issues that will be important for the department to address as it moves forward, based on work we have completed on DHS programs and operations in key areas.[1]

The creation of DHS was an enormous management challenge, representing the fusion of 22 agencies, and the size, complexity, and

[1] We supplemented our work with selected work conducted by the Department of Homeland Security Office of Inspector General. This report highlights our work on key DHS programs and efforts, but neither addresses all products that we and the DHS Office of Inspector General issued related to DHS, nor addresses all of DHS's homeland security-related activities and efforts. Also, this report focuses on our work related to DHS's homeland security efforts; it does not address other federal agencies' homeland security efforts, such as the roles the Department of Defense and intelligence agencies play in homeland security and defense.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00713 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT
67123.339

importance of the effort made the challenge especially daunting and critical to the nation's security.[2] DHS is now the third-largest federal department, with more than 200,000 employees and an annual budget of more than $50 billion. Since DHS began operations in March 2003, the department developed and refined the implementation of various policies and programs to address its homeland security missions as well as its nonhomeland security functions.[3] In particular, DHS implemented programs to secure the border and administer the immigration system; strengthen the security of the transportation sector; and prepare for and respond to terrorist threats and natural disasters. DHS also took actions to strengthen and better integrate its management functions and to transform its component agencies into a unified cabinet-level department.

We have evaluated numerous departmental programs and activities since DHS began its operations in 2003 and issued over 1,000 reports and congressional testimony in such areas as border security and immigration; transportation security; and emergency management, among others. We have made approximately 1,500 recommendations to DHS designed to improve its operations, such as to improve performance measurement efforts; strengthen management processes, including acquisition processes; enhance coordination and information sharing; and increase the use of risk information in planning and resource allocation decisions, as well as to address other key themes that have affected DHS's implementation efforts. DHS has implemented about half of these recommendations, has actions underway to address others, and has taken additional steps to strengthen its mission activities. However, we reported that the department has much to do to ensure that it conducts its missions efficiently and effectively while simultaneously preparing to

[2] These 22 agencies, offices, and programs were U.S. Customs Service; U.S. Immigration and Naturalization Service; Federal Protective Service; Transportation Security Administration; Federal Law Enforcement Training Center; Animal and Plant Health Inspection Service; Office for Domestic Preparedness; Federal Emergency Management Agency; Strategic National Stockpile and the National Disaster Medical System; Nuclear Incident Response Team; Domestic Emergency Support Team; National Domestic Preparedness Office; Chemical, Biological, Radiological, and Nuclear Countermeasures Program; Environmental Measurement Laboratory; National BW Defense Analysis Center; Plum Island Animal Disease Center; Federal Computer Incident Response Center; National Communication System; National Infrastructure Protection Center; Energy Security and Assurance Program; Secret Service; and U.S. Coast Guard.

[3] Examples of nonhomeland security functions include trade enforcement and Coast Guard search and rescue. We are including DHS's missions related to administering immigration services in this report, as these efforts have a nexus to homeland security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00714 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.340

address future challenges that face the department and the nation. Addressing these challenges will likely become increasingly complex as domestic and world events unfold, and will be particularly challenging in light of the current fiscal environment and constrained budgets.

In 2003, we designated the implementation and transformation of DHS as high risk because it represented an enormous undertaking that would require time to achieve in an effective and efficient manner.[4] Additionally, the components that merged to form DHS already faced a wide array of existing challenges, and any DHS failure to effectively carry out its mission could expose the nation to potentially serious consequences. The area has remained on our high-risk list since 2003.[5] Our prior work on mergers and organizational transformations, undertaken before the creation of DHS, found that successful transformations of large organizations, even those faced with less strenuous reorganizations than DHS, can take years to achieve.[6] Most recently, in our 2011 high-risk update, we reported that DHS took action to implement, transform, and integrate its management functions, actions that directly affect its ability to meet its homeland security and other missions.[7] For example, senior leaders at the department, including the Secretary and Deputy Secretary of Homeland Security, demonstrated strong commitment and support to addressing this high-risk area by, among other things, designating the Under Secretary for Management to be responsible for coordinating DHS's efforts to address this high-risk area, as well as other senior officials to be responsible for implementing corrective actions within each

[4] GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003). In addition to this high-risk area, DHS has responsibility for other areas we have designated as high risk. Specifically, in 2005 we designated information sharing for homeland security as high risk, involving a number of federal departments including DHS, and in 2006, we identified the National Flood Insurance Program as high risk. Further, in 2003 we expanded the scope of the high-risk area involving federal information security, which was initially designated as high risk in 1997, to include the protection of the nation's computer-reliant critical infrastructure.

[5] GAO, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).

[5] See GAO, *Highlights of a GAO Forum: Mergers and Transformations: Lessons Learned for a Department of Homeland Security and Other Federal Agencies*, GAO-03-293SP (Washington, D.C.: Nov. 14, 2002) and *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

[7] GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00715 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.341

management function. Moreover, in January 2011 DHS developed a strategy for addressing existing integration and management issues and is in the early stages of its implementation. DHS provided an update to the strategy in June 2011 that detailed plans and status updates designed to integrate and strengthen its management functions. We plan to provide the department with feedback on this update later this year. Moving forward, we reported that DHS will need to continue to implement its high-risk strategy and efforts to identify and acquire resources needed to address its risks, monitor and validate its corrective actions, and show measurable, sustainable progress in achieving key outcomes. Demonstrated, sustainable progress will be critical to helping DHS strengthen and integrate management functions within and across the department and its components.

In February 2010, DHS issued its first Quadrennial Homeland Security Review (QHSR) report, outlining a strategic framework for homeland security to guide the activities of the department and its homeland security partners, including federal, state, local, and tribal government agencies; the private sector; and nongovernmental organizations.[8] The report identified five homeland security missions—Preventing Terrorism and Enhancing Security; Securing and Managing Our Borders; Enforcing and Administering Our Immigration Laws; Safeguarding and Securing Cyberspace; and Ensuring Resilience to Disasters—and goals and objectives to be achieved within each mission. In addition to the QHSR report, in July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR), a departmentwide assessment to align DHS's programmatic activities, such as investigating drug smuggling and

[8] Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010). The Implementing Recommendations of the 9/11 Commission Act of 2007 required that beginning in 2009 and every 4 years thereafter DHS conduct a quadrennial review that provides a comprehensive examination of the homeland security strategy of the United States. Pub. L. No. 110-53, § 2401(a), 121 Stat. 266, 543-45 (2007) (codified at 6 U.S.C. § 347).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00716 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.342

inspecting cargo at ports of entry, and its organizational structure to the missions and goals identified in the QHSR.[9]

In 2007, we reported on progress made by DHS in implementing its mission and management functions by assessing actions DHS took to achieve performance expectations within each function.[10] We reported that DHS made progress in implementing all of its mission and management areas since it began operations, but progress among the areas varied significantly. For example, we reported that DHS made more progress in implementing its mission functions than its management functions. Further, among its mission functions, we reported that in implementing expectations, DHS made substantial progress in maritime security; moderate progress in aviation and surface transportation security, critical infrastructure protection, and immigration enforcement; modest progress in border security and immigration services; and limited progress in emergency preparedness and response missions.[11] We also reported on various crosscutting issues related to areas such as risk management, partnerships and coordination, and performance measurement, that had impeded DHS's implementation efforts. We further noted that DHS generally had not established quantitative goals and measures for assessing its performance and as a result, we could not

[9] Department of Homeland Security, *Bottom-Up Review Report* (Washington, D.C.: July 2010). As a result of the BUR, DHS acknowledged it had complementary department responsibilities and capabilities, which it subsequently formalized in a sixth mission published in the fiscal year 2010-2012 Annual Performance Report, known as "Providing Essential Support to National and Economic Security," to fully capture the scope of DHS's missions.

[10] GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007). We defined performance expectations as a composite of the responsibilities or functions—derived from legislation, homeland security presidential directives and executive orders, DHS planning documents, and other sources—that the department was to achieve or satisfy in implementing efforts in its mission and management areas. The performance expectations were not intended to represent performance goals or measures for the department.

[11] We defined substantial progress as DHS taking action to generally achieve more than 75 percent of the identified performance expectations; moderate progress as DHS taking action to generally achieve more than 50 percent but 75 percent or less of the identified expectations; modest progress as DHS taking action to generally achieve more than 25 percent but 50 percent or less of the identified expectations; and limited progress as DHS taking action to generally achieve 25 percent or less of the identified expectations. We found that DHS generally achieved a performance expectation if our work showed that the department had taken actions to satisfy most of the key elements of the expectation but may not have satisfied all of the elements.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00717 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.343

assess where along a spectrum of progress DHS stood in achieving its missions. Subsequent to the issuance of this report, DHS continued to take action to strengthen its operations and the management of the department, including enhancing its performance measurement efforts. Further, at the request of the Senate Committee on Homeland Security and Governmental Affairs following the issuance of our report, we provided DHS with feedback on the department's performance goals and measures as DHS worked to better position itself to assess its results. Our feedback ranged from pointing out components' limited use of outcome-oriented performance measures to assess the results or effectiveness of programs, to raising questions about the steps taken by DHS or its components to ensure the reliability and verification of performance data. Based on its internal review efforts and our feedback, DHS took action to develop and revise its performance goals and measures in an effort to strengthen its ability to assess its outcomes and progress in key mission areas. For fiscal year 2011, DHS identified 85 strategic measures for assessing its progress in achieving its QHSR missions and goals. The department plans to report on its results in meeting established targets for these new measures at the end of the fiscal year.

You asked us to review the progress made by DHS in implementing its homeland security missions since its creation after the September 11, 2001, terrorist attacks. This report addresses the following question: What progress has DHS made in implementing its mission functions since it began operations; what work, if any, remains; and what crosscutting and management issues have affected DHS's implementation efforts?

This report is based on our work on DHS since it began operations, and supplemented with work completed by the DHS Office of Inspector General (IG), with an emphasis on work completed since 2008, and updated information and documentation provided by the department in July and August 2011. It is also based on our ongoing work on key DHS programs for various congressional committees, as noted throughout the report. For this ongoing work, we examined program documentation and interviewed agency officials, among other things. Our work and the work of the DHS IG addressed many of DHS's programs, operations, and activities. This report highlights our key work in these areas, but does not address all products we and the DHS IG issued related to DHS, nor does it address all of DHS's homeland security-related activities and efforts.

To determine what progress DHS has made in implementing its mission functions and what work, if any, remains, we identified 10 DHS functional

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00718 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.344

areas, which we define as categories or areas of DHS's homeland security responsibilities. These functional areas are based on those areas we identified for DHS in our August 2007 report on DHS's progress in implementing its mission and management functions, and our analysis of DHS's QHSR and budget documents, such as its congressional budget justifications.[12] These areas include: (1) aviation security; (2) chemical, biological, radiological, and nuclear (CBRN) threats; (3) critical infrastructure protection—physical assets; (4) surface transportation security; (5) border security; (6) maritime security; (7) immigration enforcement; (8) immigration services; (9); critical infrastructure protection—cyber assets; and (10) emergency preparedness and response.[13] To identify sub-areas within these functional areas, we identified performance expectations, which we define as composites of the responsibilities or functions that the department is to achieve or satisfy based on our analysis of requirements, responsibilities, and goals set for the department by Congress, the administration, and DHS and its components. In particular, we used expectations identified in our August 2007 report as a baseline, and updated or added to these expectations by analyzing requirements and plans set forth in homeland security-related laws, presidential directives and executive orders, national strategies related to homeland security, and DHS's and components' strategic plans and documents. We then grouped these expectations within each functional area into broader sub-areas, as shown in appendix I. For example, we identified administering grant programs for surface transportation security as a performance expectation for DHS within the grants sub-area of the surface transportation functional area. Further, we then aligned our functional areas to the five QHSR missions based on our

[12] GAO-07-454.

[13] We focused these mission areas primarily on DHS's homeland security-related functions. We did not consider the U.S. Secret Service, domestic counterterrorism or intelligence activities because (1) we and the DHS IG have completed limited work in these areas; (2) there are few, if any, requirements identified for the Secret Service's mission and for DHS's role in domestic counterterrorism and intelligence (the Department of Justice serves as the lead agency for most counterterrorism initiatives); and (3) we address DHS actions that could be considered part of domestic counterterrorism and intelligence in other areas, such as aviation security, critical infrastructure protection, and border security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00719 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.345

review of the QHSR and BUR reports and DHS's fiscal year 2012 budget documents, as shown in appendix II.[14]

To identify key areas of progress and work that remains in each functional area, as well as crosscutting and management issues that have affected DHS's implementation efforts, we examined our and the DHS IG's past reports. We selected, in consultation with GAO subject matter experts, key work we and the DHS IG have completed related to the functional areas, sub-areas, and crosscutting issues. We examined the methodologies used by the DHS IG in its reports, including reviewing the scope, methodological steps, and limitations. We determined that the DHS IG reports were sufficiently reliable for the purposes of our report to provide examples, and to supplement our work, of DHS's progress and work remaining. We identified crosscutting issues based on analysis of our work in each functional mission area to determine common issues that have affected DHS's implementation efforts across the various mission areas.

We obtained and incorporated feedback on our assessments from our subject matter experts. In addition, we provided DHS with drafts of our assessments of DHS progress and work remaining in each functional area and crosscutting issue and obtained and analyzed updated information provided by DHS on these areas. In some cases, DHS provided us with updated data on its efforts, such as statistics on technology deployments or program activities. We assessed the reliability of these data by reviewing available documentation from DHS. We determined that the data were sufficiently reliable for the purposes of our report. We included updated information in our assessments, based on our review of this information and our prior work. In some cases, we could not make an assessment of the updated information DHS provided because we did not have prior work upon which to base an assessment. We noted these instances in our report.

[14] Our functional areas, as well as those key sub-areas that comprise the functional areas, may pertain to more than one QHSR mission area. In cases when sub-areas within a functional area support more than one QHSR mission, we kept the sub-area with its larger functional area and noted to which other QHSR missions it aligned. We provided DHS with our alignment of the functional areas to the QHSR missions, and incorporated the department's feedback, as appropriate.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00720 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.346

Our assessments of the progress made by DHS in functional areas and sub-areas, as well as our analyses of crosscutting issues, are based primarily on our reports, supplemented by reports of the DHS IG. As such, the assessments of progress do not reflect, nor are they intended to reflect, the extent to which DHS's actions have made the nation more secure in each area. Further, we do not intend to imply that our discussion of progress and work remaining in the functional areas and sub-areas, considered separately or together, reflect DHS's progress in implementing its missions. Instead, our assessments provide information on progress made and work that remains in key functional areas on which we have reported, as indicated by findings from our work, supplemented by that of the DHS IG. In addition, because we and the DHS IG have completed varying degrees of work (in terms of the amount and scope of reviews completed) for each functional area, and because different DHS components and offices provided us with different amounts and types of information, our assessments of DHS's progress in each area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 10 areas. Further, for some sub-areas, we were unable to make an assessment of DHS's progress because we and the DHS IG have not conducted recent work in that area or have conducted limited work. Additionally, DHS developed other performance measures against which to gauge its progress in fiscal year 2011, but has not yet reported on these measures. As such, the department did not have data available across a consistent baseline against which to assess its progress from fiscal years 2004 through 2011. Therefore, we were not able to assess DHS's progress against a baseline for each functional area and sub-area, we did not assign a qualitative rating of progress for each area, and we did not apply a weight to the expectations or sub-areas. More detailed information on those sub-areas for which we did not make an assessment is included in appendices III through XII.

We conducted this performance audit from April 2011 through September 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more detailed discussion of our scope and methodology is contained in appendix II.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00721 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.347

Background

In November 2002, the Homeland Security Act was enacted into law, creating DHS.[15] This act defined the department's missions to include preventing terrorist attacks within the United States; reducing U.S. vulnerability to terrorism; and minimizing the damages, and assisting in the recovery from, attacks that occur within the United States. The act also specified major responsibilities for the department, including to analyze information and coordinate the protection of critical infrastructure; coordinate efforts to develop countermeasures against chemical, biological, radiological, nuclear, and other emerging terrorist threats; secure U.S. borders and transportation systems; and manage the federal government's response to terrorist attacks and major disasters. Various laws have been enacted and presidential directives have been issued that, among other things, expand, modify, or clarify DHS's missions and responsibilities. For example, these laws and directives have reorganized departmental offices and functions; clarified DHS's roles and responsibilities, such as for emergency preparedness and response; and directed DHS to complete various strategic documents or implement specific programs within certain time frames. For example, the Aviation and Transportation Security Act, enacted in November 2001, established the Transportation Security Administration (TSA) and, among other things, included requirements for deploying a federal screening workforce at airports and screening all checked baggage transported on passenger aircraft using explosive detection systems.[16] The Maritime Transportation Security Act of 2002[17] and the Security and Accountability For Every Port Act of 2006 (SAFE Port Act),[18] among other things, established and modified a maritime security framework to include U.S. vessel and port facility security requirements, an international port security assessment program, and programs for scanning cargo containers. The Intelligence Reform and Terrorism Prevention Act of 2004 included provisions related to intelligence, immigration enforcement, border security, and aviation security, such as those calling for an increase in the number of Border Patrol agents and full-time investigators for violations of immigration law, subject to the availability of appropriations, and requiring DHS to develop

[15] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[16] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[17] Pub. L. No. 107-295, 116 Stat. 2064 (2002).

[18] Pub. L. No. 109-347, 120 Stat. 1884 (2006).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00722 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.348

a national strategy for transportation security.[19] The Post-Katrina Emergency Management Reform Act of 2006 required changes to the Federal Emergency Management Agency's (FEMA) organizational and management structure, and addressed other emergency management areas, such as emergency communications, and national planning and preparedness.[20] The Implementing Recommendations of the 9/11 Commission Act of 2007 includes provisions related to critical infrastructure protection, transportation security, and chemical, biological, radiological, and nuclear threats, among other areas.[21] The law references the recommendations made by the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission).

DHS began operations in March 2003, and its establishment represented a fusion of 22 federal agencies to coordinate and centralize the leadership of many homeland security activities under a single department. The department's total budget authority has increased from about $39 billion in fiscal year 2004 to about $55 billion in fiscal year 2011.[22] The department's fiscal year 2012 budget request is about $57 billion in total funding. Table 1 provides information on DHS's budget authority for each fiscal year from 2004 though 2011, as reported by DHS.

[19] Pub. L. No. 108-458, 118 Stat. 3638 (2004).

[20] Pub. L. No. 109-295, 120 Stat. 1394 (2006).

[21] Pub. L. No. 110-53, 121 Stat. 266 (2007).

[22] These data are not adjusted for inflation.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00723 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.349

Table 1: DHS Budget Authority for Fiscal Years 2004 through 2011 in Thousands of Dollars, as Reported by DHS

	Fiscal year 2004	Fiscal year 2005	Fiscal year 2006	Fiscal year 2007	Fiscal year 2008	Fiscal year 2009	Fiscal year 2010	Fiscal year 2011
U.S. Customs and Border Protection (CBP)	$5,994,287	$6,520,698	$7,970,695	$9,344,781	$10,816,001	$11,981,853	$11,846,401	$11,254,520
FEMA	$8,378,109	$74,031,032	$11,175,544	$5,223,503	$21,631,978	$10,932,016	$15,444,818	$10,462,572
U.S. Coast Guard	$7,097,405	$7,853,427	$8,782,689	$8,729,152	$9,319,760	$10,115,682	$11,150,079	$10,193,705
TSA	$4,578,043	$5,405,375	$6,167,014	$6,329,291	$6,809,359	$7,992,778	$7,656,066	$7,687,552
U.S. Immigration and Customs Enforcement (ICE)	$3,669,615	$4,244,228	$4,206,443	$4,726,641	$5,581,217	$6,054,817	$5,821,752	$5,805,420
U.S. Citizenship and Immigration Services (USCIS)	$1,549,733	$1,775,000	$1,887,850	$1,985,990	$2,902,012	$2,876,348	$2,881,597	$2,649,532
National Protection and Programs Directorate (NPPD)			$678,395	$618,577	$1,171,476	$1,188,263	$2,429,455	$2,331,197
Departmental Operations	$394,435	$527,257	$610,473	$626,123	$573,983	$859,109	$809,531	$839,291
Science and Technology Directorate (S&T)	$912,751	$1,115,450	$1,487,075	$973,109	$830,335	$932,587	$1,006,471	$827,578
Domestic Nuclear Detection Office (DNDO)				$480,968	$484,750	$514,191	$383,037	$341,744
Analysis and Operations			$252,940	$299,663	$304,500	$327,373	$333,030	$334,360
Office of Health Affairs					$118,375	$157,621	$136,850	$139,455
Office of the Inspector General	$80,318	$97,317	$84,187	$98,685	$116,711	$119,513	$134,874	$113,646

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00724 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.350

	Fiscal year 2004	Fiscal year 2005	Fiscal year 2006	Fiscal year 2007	Fiscal year 2008	Fiscal year 2009	Fiscal year 2010	Fiscal year 2011
FEMA Office of Grant Programs[a]	$4,013,182	$3,984,846	$3,377,737	$3,393,000				
United States Visitor and Immigrant Status Indicator Technology (US-VISIT)[b]	$328,053	$340,000	$336,600	$362,494				
Border and Transportation Security Directorate[b]	$8,058	$9,617						
Information Analysis and Infrastructure Protection Directorate[b]	$834,348	$887,108						
Total	**$39,374,049**	**$108,401,920**	**$48,747,645**	**$44,946,414**	**$62,584,255**	**$56,125,581**	**$62,035,217**	**$55,006,703**

Source: GAO analysis of DHS data.

Notes: Data are rounded to the nearest thousand. The data reflect total budget authority amounts as reported to us by DHS. The amounts include annual and supplemental appropriations, rescissions, amounts reprogrammed or transferred, fee estimates, and mandatory amounts. The amounts do not reflect carryover or rescissions of unobligated balances. The FEMA fiscal year 2005 amount includes about $45 billion in supplemental funding for Hurricane Katrina.

[a] The Office of Grant Programs has undergone several realignments. It was previously known as the Office of Grants and Training in the Preparedness Directorate, the Office of State and Local Government Coordination and Preparedness, and the Office for Domestic Preparedness.

[b] The Border and Transportation Security Directorate, the Information Analysis and Infrastructure Protection Directorate, and the US-VISIT program are legacy organizations within DHS. The functions of these organizations have been realigned through DHS reorganizations. In particular, in March 2007 US-VISIT was reorganized under the National Protection and Programs Directorate. The Border and Transportation Security Directorate included U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, the Transportation Security Administration, and the Federal Law Enforcement Training Center, and had budget authority in addition to those components' amounts.

A variety of factors have affected DHS's efforts to implement its mission functions since its establishment, including several departmental reorganizations. Most notably, in 2005 DHS announced the outcome of its Second Stage Review, a systematic evaluation of DHS's operations, policies, and structures. As a result of this review, the department

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00725 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.351

realigned existing directorates.[23] The Post-Katrina Emergency Management Reform Act provided for the further reorganization of functions within the department by, in particular, realigning DHS's emergency preparedness and response responsibilities.[24] Further, as a result of the Implementing Recommendations of the 9/11 Commission Act of 2007, DHS reorganized its intelligence-related operations.[25] In addition to these reorganizations, domestic and international events have affected DHS's implementation efforts. For example, Hurricanes Katrina and Rita, the 2009 H1N1 pandemic, the attempted airline attack on December 25, 2009, and the 2010 Gulf oil spill required rapid responses from the department and impacted DHS's plans and operations for mitigating vulnerabilities and addressing threats, and its progress in implementing its missions. Figure 1 provides a timeline of selected events that have affected DHS's implementation efforts.

[23] This reorganization realigned the Directorates for Border and Transportation Security, Information Analysis and Infrastructure Protection, and Emergency Response and Preparedness, and created the Directorates for Policy and Preparedness.

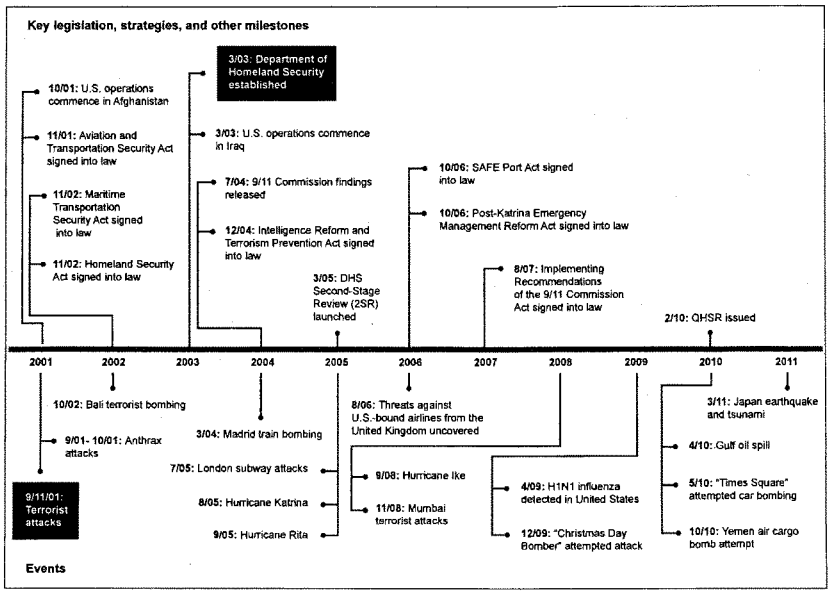
[24] Pub. L. No. 109-295, 120 Stat. 1394 (2006). Among other things, this reorganization placed certain national preparedness functions formerly in the Preparedness Directorate and legacy FEMA preparedness programs in a new National Preparedness Division within FEMA, which became responsible for policy, contingency planning, exercise coordination and evaluation, emergency management training, and hazard mitigation. In addition, the Preparedness Directorate was renamed the National Protection and Programs Directorate and retained some Preparedness Directorate elements not transferred to FEMA, such as the Office of Infrastructure Protection. Additionally, US-VISIT was moved to the new National Protection and Programs Directorate.

[25] See Pub. L. No. 110-53, 121 Stat. 266 (2007).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00726 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.352

Figure 1: Selected Events That Have Affected DHS Implementation Efforts



Source: GAO analysis of DHS data.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00727 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.353

DHS Continues to Implement and Strengthen Its Mission Functions, but Key Operational and Management Challenges Remain

Since DHS began operations in March 2003, it has developed and implemented key policies, programs, and activities for implementing its homeland security missions and functions that have created and strengthened a foundation to achieve its potential as it continues to mature. However, the department's efforts have been hindered by challenges faced in leading and coordinating the homeland security enterprise; implementing and integrating its management functions for results; and strategically managing risk and assessing, and adjusting as necessary, its homeland security efforts.[26] DHS has made progress in these three areas, but needs to take additional action, moving forward, to help it achieve its full potential.

DHS Has Made Progress in Implementing Its Mission Functions, but Program Weaknesses and Management Issues Have Hindered Implementation Efforts

DHS has made important progress in implementing and strengthening its mission functions over the past 8 years. DHS implemented key homeland security operations and achieved important goals and milestones in many areas. The department's accomplishments include developing strategic and operational plans across its range of missions; hiring, deploying and training workforces; establishing new, or expanding existing, offices and programs; and developing and issuing policies, procedures, and regulations to govern its homeland security operations. Specifically:

- DHS issued strategic and operational plans to guide its homeland security efforts, such as the QHSR, which provided a strategic framework for homeland security, and the *National Response Framework*, which is built upon coordinating structures to align key roles and responsibilities across the nation, linking all levels of government, nongovernmental organizations, and the private sector.
- DHS successfully hired, trained, and deployed workforces, such as a federal screening workforce at airports nationwide. DHS also has about 20,000 agents to patrol the U.S. land borders and about 20,600 officers to conduct screening at air, land, and sea ports of entry.
- DHS created new programs and offices, or expanded existing ones, to implement key homeland security responsibilities, such as establishing the U.S. Computer Emergency Readiness Team to, among other things, coordinate the nation's efforts to prepare for,

[26] DHS defines the homeland security enterprise as the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities, who share a common national interest in the safety and security of the United States and the American population.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00728 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.354

prevent, and respond to cyber threats to systems and communications networks. DHS also expanded programs for identifying and removing aliens subject to removal from the United States and for preventing unauthorized aliens from entering the country.

- DHS issued policies and procedures addressing, among other things, the screening of passengers at airport checkpoints, inspecting travelers seeking entry into the United States, and assessing immigration benefit applications and processes for detecting possible fraud.

Establishing these elements and others are important accomplishments and have been critical for the department to position and equip itself for fulfilling its homeland security missions and functions.

However, our work has shown that more work remains for DHS to address weaknesses in its current operational and implementation efforts and to strengthen the efficiency and effectiveness of those efforts to achieve its full potential. For example, we have reported that many DHS programs and investments have experienced cost overruns, schedule delays, and performance problems, including, for instance, DHS's recently canceled technology program for securing U.S. borders, known as the Secure Border Initiative Network, and some technologies for screening passengers at airport checkpoints. DHS also has not yet fully implemented its roles and responsibilities for developing and implementing key homeland security programs and initiatives. For example, FEMA has not yet developed a set of target capabilities for disaster preparedness or established metrics for assessing those capabilities to provide a framework for evaluating preparedness, as required by the Post-Katrina Emergency Management Reform Act of 2006.[27] Further, DHS has not yet fully deployed technologies to meet key missions for border, aviation, and maritime security. Our work has also shown that DHS should take additional action to improve the efficiency and effectiveness of a number of its programs and activities by, for example, improving program management and oversight, and better assessing homeland security requirements, needs, costs, and benefits, such as for key acquisition and technology programs.

[27] See 6 U.S.C. § 749.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00729 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.355

Table 2 provides additional information on key progress and work remaining in each of DHS's functional mission areas, as identified by our work and supplemented by that of the DHS IG, with an emphasis on work completed since 2008. We have made approximately 1,500 recommendations to DHS to help address these issues, and DHS has addressed about half of them and has actions underway to address others. Appendixes III through XII provide more detailed information on our assessment of progress made and work remaining in each functional, including recommendations we have made and the department's efforts to implement them.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00730 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.356

Table 2: Examples of Key Progress and Work Remaining in DHS's Efforts to Implement Its Homeland Security Missions on Which We Have Reported

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
Mission 1: Preventing Terrorism and Enhancing Security	Aviation security	**Key progress:** DHS has enhanced aviation security in key areas related to the aviation security workforce, passenger prescreening, passenger checkpoint screening, checked baggage security, air cargo screening, and security of airports. For example, DHS developed and implemented Secure Flight, a passenger prescreening program through which the federal government now screens all passengers on all domestic and international commercial flights to, from, and within the United States. DHS also deployed technology to screen passengers and checked baggage at airports. For example, in response to the December 25, 2009, attempted attack on Northwest flight 253, DHS revised the advanced imaging technology procurement and deployment strategy, increasing the planned deployment of advanced imaging technology from 878 to between 1,350 and 1,800 units.[a] Further, DHS is screening passengers using staff trained in behavior detection principles and has deployed about 3,000 Behavior Detection Officers to 161 airports as part of its Screening of Passengers by Observation Techniques program. Moreover, DHS reported, as of August 2010, that it had established a system to screen 100 percent of domestic air cargo (cargo transported within and outbound from the United States) transported on passenger aircraft by, among other things, creating a voluntary program to facilitate screening throughout the air cargo supply chain and taking steps to test technologies for screening air cargo. **What remains to be done:** DHS should take additional action to strengthen its aviation security efforts. For example, a risk-based strategy and a cost-benefit analysis of airport checkpoint technologies would improve passenger checkpoint screening. TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based and did not reflect some of the key risk management principles, such as conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and including a cost-benefit analysis and performance measures. Further, in March 2010, we reported that it was unclear whether the advanced imaging technology would have detected the weapon used in the December 25, 2009, attempted terrorist attack based on the preliminary testing information we received. DHS also had not validated the science supporting its Screening of Passengers by Observation Techniques program, or determined if behavior detection techniques could be successfully used across the aviation system to detect threats before deploying the program. DHS completed a program validation study in April 2011 which found that the program was more effective than random screening, but that more work was needed to determine whether the science could be used for counterterrorism purposes in the aviation environment. Moreover, DHS does not yet have a plan and schedule for deploying checked baggage screening technologies to meet recently enhanced explosive detection requirements. In addition, DHS does not yet have a mechanism to verify the accuracy of domestic and inbound air cargo screening data to help ensure that screening is being conducted at reported levels, and DHS does not yet have approved technology to screen cargo once it is loaded onto a pallet or container—both of which are common means of transporting air cargo on passenger aircraft, thus requiring that screening occur before incorporation into pallets and containers.	Appendix III

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00731 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.357

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
	CBRN threats	**Key progress:** DHS made progress in assessing risks posed by CBRN threats, developing CBRN detection capabilities, and planning for nuclear detection. For example, DHS develops risk assessments of CBRN threats and has issued seven classified CBRN risk assessments since 2006.[b] DHS also assessed the threat posed by specific CBRN agents in order to determine which of those agents pose a material threat to the United States, known as material threat assessments. With regard to CBRN detection capabilities, DHS implemented the BioWatch program in more than 30 metropolitan areas to detect specific airborne biological threat agents. Further, DHS established the National Biosurveillance Integration Center to enhance the federal government's capability to identify and track biological events of national concern. In addition, DHS coordinated the development of a strategic plan for the global nuclear detection architecture—a multidepartment effort to protect against terrorist attacks using nuclear and radiological materials through coordinated activities—and has deployed radiation detection equipment. **What remains to be done:** More work remains for DHS to strengthen its CBRN assessment, detection, and mitigation capabilities. For example, DHS should better coordinate with the Department of Health and Human Services in conducting CBRN risk assessments by developing written policies and procedures governing development of the assessments. Moreover, the National Biosurveillance Integration Center lacks resources necessary for operations, such as data and personnel from its partner agencies. Additionally, work remains for DHS in its implementation of the global nuclear detection architecture. Specifically, the strategic plan for the architecture did not include some key components, such as funding needed to achieve the strategic plan's objectives, or monitoring mechanisms for determining programmatic progress and identifying needed improvements. DHS officials told us that they will address these missing elements in an implementation plan, which they plan to issue by the end of 2011.	Appendix IV
	Critical infrastructure protection—physical assets	**Key progress:** DHS expanded its efforts to conduct risk assessments and planning, provide for protection and resiliency, and implement partnerships and coordination mechanisms for physical critical assets. For example, DHS updated the *National Infrastructure Protection Plan* to include an emphasis on resiliency (the capacity to resist, absorb, or successfully adapt, respond to, or recover from disasters), and an enhanced discussion about DHS risk management. Moreover, DHS components with responsibility for critical infrastructure sectors, such as transportation security, have begun to use risk-based assessments in their critical infrastructure related planning and protection efforts. Further, DHS has various voluntary programs in place to conduct vulnerability assessments and security surveys at and across facilities from the 18 critical infrastructure sectors, and uses these assessments to develop and disseminate information on steps asset owners and operators can take to protect their facilities. In addition, DHS coordinated with critical infrastructure stakeholders, including other federal regulatory authorities to identify overlaps and gaps in critical infrastructure security activities.	Appendix V

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00732 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.358

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		What remains to be done: Additional actions are needed for DHS to strengthen its critical infrastructure protection programs and efforts. For example, DHS has not fully implemented an approach to measure its effectiveness in working with critical asset owners and operators in their efforts to take actions to mitigate resiliency gaps identified during various vulnerability assessments. Moreover, DHS components have faced difficulties in incorporating risk-based assessments in critical infrastructure planning and protection efforts, such as in planning for security in surface transportation modes like highway infrastructure. Further, DHS should determine the feasibility of developing an approach to disseminating information on resiliency practices to its critical infrastructure partners to better position itself to help asset owners and operators consider and adopt resiliency strategies, and provide them with information on potential security investments.	
	Surface transportation security	**Key progress:** DHS expanded its efforts in key surface transportation security areas, such as risk assessments and strategic planning; the surface transportation inspector workforce; and information sharing. For example, DHS conducted risk assessments of surface transportation modes and developed a transportation sector security risk assessment that assessed risk within and across the various modes. Further, DHS more than doubled its surface transportation inspector workforce and, as of July 2011, reported that its surface inspectors had conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, among other things. Moreover, DHS allocates transit grant funding based on risk assessments and has taken steps to measure performance of its Transit Security Grant Program, which provides funds to owners and operators of mass transit and passenger rail systems. In addition, DHS expanded its sharing of surface transportation security information by, among other things, establishing information networks. **What remains to be done:** DHS should take further action to strengthen its surface transportation security programs and operations. For example, DHS's efforts to improve elements of risk assessments of surface transportation modes are in the early stages of implementation. Moreover, DHS noted limitations in its transportation sector security risk assessment—such as the exclusion of threats from lone wolf operators—that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. Further, DHS has not yet completed a long-term workforce plan that identifies future needs for its surface transportation inspector workforce. It also has not yet issued regulations for a training program for mass transit, rail, and bus employees, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[c] Additionally, DHS's information sharing efforts would benefit from improved streamlining, coordination, and assessment of the effectiveness of information sharing mechanisms.	Appendix VI

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00733 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.359

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
Mission 2: Securing and Managing Our Borders	Border security	**Key progress:** DHS expanded its efforts in key border security areas, such as inspection of travelers and cargo at ports of entry, security of the border between ports of entry, visa adjudication security, and collaboration with stakeholders. Specifically, DHS has undertaken efforts to keep terrorists and other dangerous people from entering the country. For example, DHS implemented the US-VISIT program to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information. DHS established plans for, and had begun to interact with and involve stakeholders in, developing an exit capability. DHS deployed technologies and other infrastructure to secure the border between ports of entry, including more than 600 miles of tactical infrastructure, such as fencing, along the border. DHS also improved programs designed to enhance the security of documents used to enter the United States. For example, DHS deployed the Visa Security Program, in which DHS personnel review visa applications to help prevent individuals who pose a threat from entering the United States, to 19 posts in 15 countries, and developed a 5-year expansion plan for the program. In addition, DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts through, among other things, the establishment of interagency forums. **What remains to be done:** More work remains for DHS to strengthen its border security programs and operations. For example, although it has developed a plan, DHS has not yet adopted an integrated approach to scheduling, executing, and tracking the work needed to be accomplished to deliver a comprehensive biometric exit solution as part of the US-VISIT program. Further, DHS experienced schedule delays and performance problems with its information technology program for securing the border between ports of entry—the Secure Border Initiative Network—which led to its cancellation. Because of the program's decreased scope, uncertain timing, unclear costs, and limited life cycle management, it was unclear whether DHS's pursuit of the program was cost-effective. DHS is transitioning to a new approach for border technology, which we are assessing. With regard to the Visa Security Program, DHS did not fully follow or update its 5-year expansion plan. For instance, it did not establish 9 posts identified for expansion in 2009 and 2010, and had not taken steps to address visa risk at posts that did not have a Visa Security Program presence. Additionally, DHS should strengthen its oversight of interagency forums operating along the northern border.	Appendix VII

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00734 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.360

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
	Maritime security	**Key progress:** DHS expanded its efforts in key maritime security areas, such as port facility and vessel security, maritime security domain awareness and information sharing, and international supply chain security. For example, DHS strengthened risk management through the development of a risk assessment model, and addressed risks to port facilities through annual inspections in which DHS identified and corrected deficiencies, such as facilities failing to follow security plans for access control. Further, DHS took action to address risks posed by foreign seafarers entering U.S. seaports by, for example, conducting advance screening before the arrival of vessels at U.S. ports, inspections, and enforcement operations. DHS developed the Transportation Worker Identification Credential program to manage the access of unescorted maritime workers to secure areas of regulated maritime facilities. DHS also implemented measures to help secure passenger vessels including cruise ships, ferries, and energy commodity vessels such as tankers, including assessing risks to these types of vessels. Moreover, for tracking vessels at sea, the Coast Guard uses a long-range identification and tracking system, and a commercially provided long-range automatic identification system.[d] For tracking vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system, and also either operates, or has access to, radar and cameras in some ports. DHS also developed a layered security strategy for cargo container security, including deploying screening technologies and partnering with foreign governments. **What remains to be done:** DHS should take additional action to strengthen its maritime security efforts. For example, because of a lack of technology capability, DHS does not electronically verify identity and immigration status of foreign seafarers, as part of its onboard admissibility inspections of cargo vessels, thus limiting the assurance that fraud could be identified among documents presented by them. In addition, the Transportation Worker Identification Credential program's controls were not designed to provide reasonable assurance that only qualified applicants acquire credentials. For example, during covert tests of the Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Moreover, DHS has not assessed the costs and benefits of requiring cruise lines to provide passenger reservation data for screening, which could help improve identification and targeting of potential terrorists. Further, the vessel tracking systems used in U.S. coastal areas, inland waterways, and ports had more difficulty tracking smaller and noncommercial vessels because these vessels were not generally required to carry automatic identification system equipment, and because of the technical limitations of radar and cameras. In addition, DHS has made limited progress in scanning containers at the initial ports participating in the Secure Freight Initiative, a program at selected ports with the intent of scanning 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas, leaving the feasibility of 100 percent scanning largely unproven. CBP has not yet developed a plan for full implementation of a statutory requirement that 100 percent of U.S.-bound container cargo be scanned by 2012.[e]	Appendix VIII

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00735 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.361

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
Mission 3: Enforcing and Administering Our Immigration Laws	Immigration enforcement	**Key progress:** DHS expanded its immigration and customs enforcement programs and activities in key areas such as overstay enforcement, compliance with workplace immigration laws, alien smuggling, and firearms trafficking. For example, DHS increased its resources for investigating overstays (unauthorized immigrants who entered the United States legally on a temporary basis then overstayed their authorized periods of admission) and alien smuggling operations, and deployed border enforcement task forces to investigate illicit smuggling of people and goods, including firearms. In addition, DHS took action to improve the E-Verify program, which provides employers a voluntary tool for verifying an employee's authorization to work in the United States, by, for example, increasing the program's accuracy by expanding the number of databases it can query. Further, DHS expanded its programs and activities to identify and remove criminal aliens in federal, state, and local custody who are eligible for removal from the United States by, for example, entering into agreements with state and local law enforcement agencies to train officers to assist in identifying those individuals who are in the United States illegally. **What remains to be done:** Key weaknesses remain in DHS's immigration and customs enforcement efforts. For example, DHS took action to address a small portion of the estimated overstay population in the United States, and lacks measures for assessing its progress in addressing overstays. In particular, DHS field offices had closed about 34,700 overstay investigations assigned to them from fiscal year 2004 through 2010, as of October 2010; these cases resulted in approximately 8,100 arrests, relative to a total estimated overstay population of 4 million to 5.5 million.[f] Additionally, we reported that since fiscal year 2006, U.S. Immigration and Customs Enforcement within DHS allocated about 3 percent of its investigative work hours to overstay investigations. Moreover, DHS should better leverage opportunities to strengthen its alien smuggling enforcement efforts by assessing the possible use of various investigative techniques, such as those that follow cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. Further, weaknesses with the E-Verify program, including challenges in accurately estimating E-Verify costs, put DHS at an increased risk of not making informed investment decisions.	Appendix IX
	Immigration services	**Key progress:** DHS improved the quality and efficiency of the immigration benefit administration process, and expanded its efforts to detect and deter immigration fraud. For example, DHS initiated efforts to modernize its immigration benefit administration infrastructure; improve the efficiency and timeliness of its application intake process; and ensure quality in its benefit adjudication processes. Further, DHS designed training programs and quality reviews to help ensure the integrity of asylum adjudications. Moreover, in 2004 DHS established the Office of Fraud Detection and National Security, now a directorate, to lead immigration fraud detection and deterrence efforts, and this directorate has since developed and implemented strategies for this purpose.	Appendix X

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00736 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.362

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		What remains to be done: More work remains in DHS's efforts to improve its administration of immigration benefits. For example, DHS's program for transforming its immigration benefit processing infrastructure and business practices from paper-based to digital systems missed its planned milestones by more than 2 years, and has been hampered by management challenges, such as insufficient planning and not adhering to DHS acquisition guidance before selecting a contractor to assist with implementation of the transformation program. Additionally, while the Fraud Detection and National Security Directorate put in place strategies for detecting and deterring immigration fraud, DHS should take additional action to address vulnerabilities identified in its assessments intended to determine the extent and nature of fraud in certain applications. Further, despite mechanisms DHS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers we surveyed cited challenges in identifying fraud as a key factor affecting their adjudications. For example, 73 percent of asylum officer survey respondents reported it was moderately or very difficult to identify document fraud.	
Mission 4: Safeguarding and Securing Cyberspace	Critical infrastructure protection—cyber assets	**Key progress:** DHS expanded its efforts to conduct cybersecurity risk assessments and planning, provide for the protection and resilience of cyber assets, and implement cybersecurity partnerships and coordination mechanisms. For example, DHS developed the first National Cyber Incident Response Plan in September 2010 to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels. DHS also took steps to secure external network connections in use by the federal government by establishing the National Cybersecurity Protection System, operationally known as Einstein, to analyze computer network traffic information to and from agencies. In 2008, DHS developed Einstein 2, which incorporated network intrusion detection technology into the capabilities of the initial version of the system. Additionally, the department made progress in enhancing its cyber analysis and incident warning capabilities through the establishment of the U.S. Computer Emergency Readiness Team, which, among other things, coordinates the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. Moreover, since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing lessons it had learned from this exercise to strengthen public and private incident response capabilities.	Appendix XI

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00737 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.363

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		What remains to be done: Key challenges remain in DHS's cybersecurity efforts. For example, to expand its protection and resiliency efforts, DHS needs to lead a concerted effort to consolidate and better secure Internet connections at federal agencies. Further, DHS faced challenges regarding deploying Einstein 2, including understanding the extent to which its objective was being met because the department lacked performance measures that addressed whether agencies report whether the alerts represent actual incidents. DHS also faces challenges in fully establishing a comprehensive national cyber analysis and warning capability. For example, the U.S. Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities. These attributes are related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For instance, the U.S. Computer Emergency Readiness Team provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. Additionally, expectations of private sector stakeholders are not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.	
Mission 5: Ensuring Resilience to Disasters	Emergency preparedness and response	**Key progress:** DHS expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; and enhanced emergency communications. For example, DHS developed various plans for disaster preparedness and response. In particular, in 2004 DHS issued the *National Response Plan* and subsequently made revisions to it, culminating in the issuance of the *National Response Framework* in January 2008, which outlines the guiding principles and major roles and responsibilities of government, nongovernmental organizations, and private sector entities for response to disasters of all sizes and causes. Further, DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-based preparedness, and a Target Capabilities List, designed to provide a national-level generic model of capabilities defining all-hazards preparedness. DHS also assisted local communities with developing long-term disaster recovery plans as part of its post-disaster assistance. For example, DHS assisted Iowa City's recovery from major floods in 2008 by, among other things, identifying possible federal funding sources for specific projects in the city's recovery plan, and advising the city on how to prepare effective project proposals. DHS is also finalizing a National Disaster Recovery Framework, intended to provide a model to identify and address challenges that arise during the disaster recovery process. Moreover, DHS issued the National Emergency Communications Plan—the first strategic document for improving emergency communications nationwide.	Appendix XII

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00738 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.364

QHSR mission	Functional area	Summary of key progress and work remaining	Appendix
		What remains to be done: More work remains in DHS's efforts to assess capabilities for all-hazards preparedness and provide long-term disaster recovery assistance. For example, DHS has not yet developed national preparedness capability requirements based on established metrics to provide a framework for assessing preparedness. Further, the data DHS collected to measure national preparedness were limited by reliability and measurement issues related to the lack of standardization. Until a framework for assessing preparedness is in place, DHS will not have a basis on which to operationalize and implement its conceptual approach for assessing local, state, and federal preparedness capabilities against capability requirements and identify capability gaps for prioritizing investments in national preparedness. Moreover, with regard to long-term disaster recovery assistance, DHS's criteria for when to provide the assistance were vague, and, in some cases, DHS provided assistance before state and local governments had the capacity to work effectively with DHS. Additionally, DHS should improve the efficacy of the grant application and review process by mitigating duplication or redundancy within the various preparedness grant programs. Until DHS evaluates grant applications across grant programs, DHS cannot ascertain whether or to what extent multiple funding requests are being submitted for similar purposes.	

Source: GAO analysis based on the areas included in this report.

Note: This table also includes examples from selected DHS IG reports.

[a] Advanced imaging technology units produce an image of a passenger's body that DHS personnel use to look for anomalies, such as explosives or other prohibited items.

[b] DHS issued three bioterrorism risk assessments in 2006, 2008, and 2010; two chemical terrorism risk assessments in 2008 and 2010; and two integrated CBRN terrorism risk assessments in 2008 and 2011. DHS also plans to issue the first radiological and nuclear terrorism risk assessment in 2011.

[c] The Implementing Recommendations of the 9/11 Commission Act of 2007 requires TSA to issue regulations for a training program to prepare mass transit, rail, and over-the-road bus employees for potential security threats and conditions. 6 U.S.C. §§ 1137, 1167, 1184.

[d] The International Maritime Organization is the international body responsible for improving maritime safety. The organization primarily regulates maritime safety and security through the *International Convention for the Safety of Life at Sea, 1974*. In 2006, amendments to this treaty were adopted that mandated the creation of an international long-range identification and tracking system that, in general, requires the International Maritime Organization member state vessels on international voyages to transmit certain information; the creation of data centers that will, among other roles, receive long-range identification and tracking system information from the vessels; and an information exchange network, centered on an international data exchange for receiving and transmitting long-range identification and tracking information to authorized nations.

[e] See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)).

[f] According to our April 2011 report, the most recent estimates from the Pew Hispanic Center approximated that, in 2006, out of an unauthorized resident alien population of 11.5 million to 12 million in the United States, about 4 million to 5.5 million were overstays. Pew Hispanic Center, *Modes of Entry for the Unauthorized Migrant Population* (Washington, D.C.: May 22, 2006).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00739 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.365

Impacting the department's ability to efficiently and effectively satisfy its missions are:

- the need to integrate and strengthen its management functions;
- the need for increased utilization of performance assessments;
- the need for an enhanced use of risk information to inform planning, programming, and investment decision-making;
- limitations in effective sharing and use of terrorism-related information;
- partnerships that are not sustained or fully leveraged; and
- limitations in developing and deploying technologies to meet mission needs.

DHS made progress in addressing these areas, but more work is needed, going forward, to further mitigate these challenges and their impact on DHS's mission implementation. As we have previously reported, while it is important that DHS continue to work to strengthen each of its functional areas, it is equally important that these areas be addressed from a comprehensive, departmentwide perspective to help mitigate longstanding issues that have impacted the department's progress.

Table 3 provides examples of crosscutting issues that have impacted the department's progress, as identified by our work. Appendixes XIII through XVIII provide more detailed information on our assessment of progress made and work remaining in each crosscutting area, including recommendations we have made and DHS's efforts to implement them.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00740 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.366

Table 3: Crosscutting and Management Issues Affecting DHS's Progress in Implementing Its Homeland Security Missions

Crosscutting issue	Summary of key progress and work remaining	Appendix
DHS transformation and implementation	DHS has taken action to strengthen its management functions, including its acquisition, information technology, financial, and human capital management functions. DHS developed a strategy to help address these issues that includes corrective actions for mitigating its management challenges. However, DHS needs to demonstrate sustainable, measurable progress in implementing the strategy and corrective actions to address challenges we have identified within and across its management functions, as the effectiveness of these functions and their implementation affect its ability to fulfill its homeland security and other missions.	Appendix XIII
Performance measurement	DHS strengthened its performance measures in recent years and linked its measures to the QHSR's missions and goals. However, DHS and its components have not yet fully developed measures for assessing the effectiveness of key homeland security programs, such as programs for securing the border and preparing the nation for emergency incidents. While improvements have been made, the department needs to continue to work to strengthen its measures to more fully assess the effectiveness and results of its programs and efforts to inform any needed adjustments.	Appendix XIV
Risk management	DHS and its component agencies developed strategies and tools for conducting risk assessments. However, the department needs to strengthen its use of risk information to inform its planning and investment decision-making. For example, DHS could better use risk information to plan and prioritize security measures and investments within and across its mission areas, as the department cannot secure the nation against every conceivable threat.	Appendix XV
Information sharing	DHS expanded its efforts to share terrorism-related information, particularly with state and local government and private sector entities, and has initiatives underway to identify state and local partners' information needs. However, DHS could take further actions to more comprehensively identify state and local agencies' information sharing needs, establish performance measures for assessing results, and streamline its mechanisms for sharing information. Effectively sharing terrorism-related information with state and local law enforcement agencies is important, as they depend on such information to maintain situational awareness of emerging threats and to help allocate homeland security resources.	Appendix XVI
Partnerships and coordination	DHS made progress in coordinating its programs and activities with homeland security partners, but could strengthen its efforts to ensure that partners' information and other needs are met and provide enhanced oversight of coordination mechanisms. For example, with regard to border security, federal, state, local, tribal, and Canadian law enforcement partners reported improved DHS coordination to secure the northern border through mechanisms such as interagency forums that helped to establish a common understanding of border security threats. However, these partners cited ongoing challenges in sharing information and resources for daily border security related to operations and investigations.	Appendix XVII
Developing and deploying new technologies for homeland security	DHS took action to develop and deploy new technologies to help meet its homeland security missions. However, in a number of instances DHS pursued acquisitions without ensuring that the technologies met defined requirements, conducting and documenting appropriate testing and evaluation, and performing cost-benefit analyses, resulting in important technology programs not meeting performance expectations.	Appendix XVIII

Source: GAO analysis based on the areas included in this report.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00741 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.367

Key Themes Have Impacted DHS's Progress in Implementing Its Mission Functions

Our work on the functional mission areas and crosscutting issues discussed in this report has identified several key themes—leading and coordinating the homeland security enterprise, implementing and integrating management functions for results, and strategically managing risks and assessing homeland security efforts—that have impacted the department's progress since it began operations. These themes provide insights that can inform DHS's efforts, moving forward, as it works to implement its missions within a dynamic and evolving homeland security environment, one in which a broad range of threats face the nation—from terrorists' possible use of a chemical or biological agent to carry out an attack to cyber threats and intrusions to natural disasters and infectious diseases. DHS made progress and had successes in all of these areas, but our work found that these themes have been at the foundation of DHS's implementation challenges, and need to be addressed from a departmentwide perspective to position DHS for the future and enable it to satisfy the expectations set for it by the Congress, the administration, and the country.

Leading and coordinating the homeland security enterprise. While DHS is one of a number of entities with a role in securing the homeland, it has significant leadership and coordination responsibilities for managing efforts across the homeland security enterprise. To satisfy these responsibilities, it is critically important that DHS develop, maintain and leverage effective partnerships with its stakeholders, while at the same time addressing DHS-specific responsibilities in satisfying its missions. Before DHS began operations, we reported that the quality and continuity of the new department's leadership would be critical to building and sustaining the long-term effectiveness of DHS and achieving homeland security goals and objectives. In particular, we reported that top leadership involvement and clear lines of accountability for making improvements would be critical to marshalling the needed resources and building and maintaining organizationwide commitment to new ways of doing business. We further reported that to secure the nation, DHS must form effective and sustained partnerships between components and also with a range of other entities, including federal agencies; state, local, and tribal governments; the private and nonprofit sectors; and international partners. Critical aspects of DHS's success depend on well-functioning relationships with third parties, and DHS needs to continue to create and maintain a structure that can leverage partnerships to effectively implement homeland security efforts. Eight years after its establishment, DHS has made important strides in providing leadership and coordinating efforts across the enterprise as it continues to work to implement and strengthen its effectiveness across its range of missions. For example,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00742 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.368

DHS strengthened its partnerships and collaboration w ith foreign governments to coordinate and standardize security practices for aviation security. It has also improved coordination and clarified roles and responsibilities with state, local, and tribal governments for emergency management. In addition, DHS operates the Protective Security Advisor Program, which deploys critical infrastructure protection and security specialists to local communities to help foster effective information sharing with the private sector and local communities.

However, our work has found that DHS made limited progress in forging effective partnerships and sharing information throughout the enterprise early in its existence and as it matured, and although DHS continues to make improvements in this area, it faces challenges in building and leveraging these partnerships and information. These challenges have impeded the department's progress, affecting its ability to effectively and efficiently satisfy its missions. For example, we found that DHS has not effectively overseen key interagency forums its components have established with other federal, state, local, tribal, and foreign law enforcement agencies to secure the border, raising the risk of duplication, overlap, and an inefficient use of resources.

In 2005 we designated information sharing for homeland security, for which DHS has key responsibilities, as high risk because the federal government faced serious challenges in analyzing information and sharing it among partners in a timely, accurate, and useful way to protect against terrorist threats. We reported that DHS must effectively share terrorism-related information with state and local law enforcement agencies because they depend on it to maintain awareness of emerging threats and to allocate homeland security resources, among other things. Further, gaps in sharing, such as agencies' failure to link information about the individual who attempted to conduct the December 25, 2009, airline bombing, prevented the individual from being included on the federal government's consolidated terrorist watchlist, a tool used by DHS to screen for persons who pose a security risk.

The federal government and DHS have made progress in this area, but more work remains to strengthen and streamline existing information sharing mechanisms and better address partners' information needs. These gaps have contributed to, among other things, DHS not realizing the full potential and contributions that its partners can provide, and not maximizing its effectiveness in achieving its missions. For example, with regard to cybersecurity, private sector stakeholders reported that they expect their federal partners, including DHS, to provide usable, timely,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00743 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.369

and actionable cyber threat information and alerts and a secure mechanism for sharing information, among other things. However, according to private sector stakeholders, federal partners are not consistently meeting these expectations. Without improvements in meeting private and public sector expectations for sharing cyber threat information, private-public partnerships will remain less than optimal, and there is a risk that owners of critical infrastructure will not have the information and mechanisms needed to thwart sophisticated cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure. Moreover, we have identified the potential for overlap between various mechanisms DHS uses for sharing security-related information with public transit agencies. DHS needs to continue to streamline its mechanisms for sharing information with public transit agencies to reduce the volume of similar information these agencies receive from DHS, making it easier for them to discern relevant information and take appropriate actions to enhance security. Moving forward, it will be important that DHS continue to enhance its focus and efforts to strengthen and leverage the broader homeland security enterprise, and build off the important progress that it has made thus far. In addressing ever changing and complex threats, and with the vast array of partners with which DHS must coordinate, continued leadership and stewardship will be critical in achieving this end.

Implementing and integrating management functions for results. Following its establishment, the department focused its efforts primarily on implementing its various missions to meet pressing homeland security needs and threats, and less on creating and integrating a fully and effectively functioning department from 22 disparate agencies. This initial focus on mission implementation was understandable given the critical homeland security needs facing the nation after the department's establishment, and the enormous challenge posed by creating, integrating, and transforming a department as large and complex as DHS. As the department matured, it has put into place management policies and processes and made a range of other enhancements to its management functions—acquisition, information technology, financial, and human capital management.[28] However, the department has not effectively executed these processes in a number of instances, across the

[28] For example, in 2010 DHS published an acquisition management directive, which established an oversight framework to manage acquisition programs.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00744 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.370

range of its management functions, and has not fully integrated these functions across components and among departmental missions. These issues have contributed to performance problems in programs aimed at delivering important mission capabilities. For example, DHS did not sufficiently define what capabilities and benefits would be delivered, by when, and at what cost for US-VISIT—which is to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information—and has not yet reached a decision on deploying an exit capability. Not defining these capabilities and benefits contributed to development and deployment delays. In another example, with respect to the cargo advanced automated radiography system to detect certain nuclear materials in vehicles and containers at ports, DHS pursued the acquisition and deployment of the system without fully understanding that it would not fit within existing inspection lanes at ports of entry. DHS subsequently canceled this program.

In 2003, GAO designated the transformation and implementation of DHS as high risk because the department had to transform 22 agencies—several with major management challenges—into one department, and failure to effectively address DHS's management and mission risks could have serious consequences for U.S. national and economic security. Eight years later, DHS remains on our high-risk list. DHS has made important strides in working to strengthen its management functions, has established plans to strengthen and integrate these functions, and in recent years has demonstrated strong leadership support to address these long-standing issues. In particular, DHS developed various management policies, directives, and governance structures, such as acquisition and information technology management policies and controls, to provide enhanced guidance on investment decision-making. DHS also reduced its financial management material weaknesses in internal control over financial reporting and developed strategies to strengthen human capital management, such as its *Workforce Strategy for Fiscal Years 2011-2016*. However, more work remains to position these management areas for success. For example, DHS does not yet have enough skilled personnel to carry out activities in some key programmatic and management areas, such as for acquisition management, and was ranked 28 out of 32 agencies in the 2010 Partnership for Public Service's Best Places to Work in the Federal

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00745 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.371

Government rankings.[29] DHS also has not yet implemented an integrated financial management system, impeding its ability to have ready access to information to inform decision-making, and has been unable to obtain a clean audit opinion on the audit of its consolidated financial statements since its establishment. Moving forward, addressing these management challenges will be critical for DHS's success, as will the integration of these functions across the department to achieve efficiencies and effectiveness.

Strategically managing risks and assessing homeland security efforts. Forming a new department while working to implement statutorily mandated and department-initiated programs and initiatives, and responding to adapting adversaries and evolving threats was and is a significant challenge facing DHS. Key threats and incidents that have emerged, both domestically and internationally, such as the anthrax attacks, Hurricanes Katrina and Rita, and a number of attempted attacks against the aviation sector, have impacted and altered the department's approaches and investments. For example, DHS made key changes to its processes and technology investments for screening passengers and baggage at airports in part as a result of threats facing commercial aviation. DHS also changed its processes and clarified roles and responsibilities for emergency management in the aftermath of Hurricanes Katrina and Rita.

It is understandable that these events and threats had to be addressed as they arose. However, our work has shown, throughout the department, that limited strategic and program planning, as well as assessment and evaluation to inform approaches and investment decisions, have contributed to programs not meeting strategic needs or doing so effectively and efficiently. For example, as we reported in July 2011, the Coast Guard's planned acquisitions through its Deepwater Program, which began before DHS's creation and includes efforts to build or modernize ships and aircraft and supporting capabilities that are critical to meeting the Coast Guard's core missions in the future, is unachievable due to cost growth, schedule delays, and affordability issues. In addition, because FEMA has not yet developed a set of target disaster preparedness capabilities and a systematic means of assessing those

[29] Partnership for Public Service and the Institute for the Study of Public Policy Implementation at the American University School of Public Affairs, *The Best Places to Work in the Federal Government* (Washington, D.C.: 2010).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00746 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.372

capabilities, as required by the Post-Katrina Emergency Management Reform Act of 2006 and Presidential Policy Directive 8: National Preparedness, it cannot effectively evaluate and identify key capability gaps and target limited resources to fill those gaps. We have also reported that while DHS has made important progress in assessing and analyzing risk across sectors, it has more work to do in using this information to inform planning and resource allocation decisions. Risk management has been widely supported by Congress and DHS as a management approach for homeland security, enhancing the department's ability to make informed decisions and prioritize resource investments. Since DHS does not have unlimited resources and cannot protect the nation from every conceivable threat, it must make risk-informed decisions regarding its homeland security approaches and strategies.

Moreover, we have reported on the need for enhanced performance assessment, that is, evaluating existing programs and operations to determine whether they are operating as intended or are in need of change, across DHS's missions. Information on the performance of programs is critical for helping the department, the Congress, and other stakeholders more systematically assess strengths and weaknesses and inform decision-making. In recent years, DHS has placed an increased emphasis on strengthening its mechanisms for assessing the performance and effectiveness of its homeland security programs. For example, DHS established new performance measures, and modified existing ones, to better assess many of its programs and efforts. Enhanced assessment of programs' performance and the use of that information to inform decisions will provide the department with important insights in determining the extent to which programs and operations are meeting intended goals and results and at what cost.

However, our work has found that DHS continues to miss opportunities to optimize performance across its missions because of a lack of reliable performance information or assessment of existing information; evaluation of feasible alternatives; and, as appropriate, adjustment of programs or operations that are not meeting mission needs. For example, TSA's program for research, development, and deployment of passenger checkpoint screening technologies lacked a risk-based plan and performance measures to assess the extent to which checkpoint screening technologies were achieving the program's security goals, and thereby reducing or mitigating the risk of terrorist attacks. As a result, TSA had limited assurance that its strategy targeted the most critical risks and that it was investing in the most cost-effective new technologies or other

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00747 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.373

protective measures. Further, with regard to border security efforts, CBP established performance measures for its checkpoints to indicate checkpoint contributions toward apprehending removable aliens and seizing illegal drugs, but the lack of information on those passing through checkpoints undetected continued to challenge CBP's ability to measure checkpoint effectiveness and provide public accountability. As the department further matures and seeks to optimize its operations, DHS will need to look beyond immediate requirements; assess programs' sustainability across the long term, particularly in light of constrained budgets; and evaluate tradeoffs within and among programs across the homeland security enterprise. Doing so should better equip DHS to adapt and respond to new threats in a sustainable manner as it works to address existing ones.

Concluding Observations

Given DHS's role and leadership responsibilities in securing the homeland, it is critical that the department's programs and activities are operating as efficiently and effectively as possible, that these programs are sustainable, and that they continue to mature, evolve, and adapt to address pressing security needs. DHS has made significant progress throughout its missions since its creation, but more work is needed to further transform the department into a more integrated and effective organization. Specifically, DHS has taken many actions to (1) develop strategic and operational plans across its range of missions; (2) hire, deploy and train workforces; (3) establish new, or expand existing, offices and programs; and (4) develop and issue policies, procedures, and regulations to govern its homeland security operations. DHS has also made important progress in strengthening partnerships with stakeholders, improving its management processes and sharing of information, and enhancing its risk management and performance measurement efforts. These accomplishments are especially noteworthy given that the department has had to work to transform itself into a fully functioning cabinet department while implementing its missions—a difficult undertaking for any organization and one that can take years to achieve even under less daunting circumstances.

Impacting the department's efforts have been a variety of factors and events, such as attempted terrorist attacks and natural disasters, as well as new responsibilities and authorities provided by Congress and the administration. These events collectively have forced DHS to continually reassess its priorities and reallocate resources as needed, and have impacted its continued integration and transformation. Given the nature of DHS's mission, the need to remain nimble and adaptable to respond to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00748 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.374

evolving threats, as well as to work to anticipate new ones, will not change and may become even more complex and challenging as domestic and world events unfold, particularly in light of reduced budgets and constrained resources. To better position itself to address these challenges, our work has shown that DHS should place an increased emphasis and take additional action in supporting and leveraging the homeland security enterprise, managing its operations to achieve needed results, and strategically planning for the future while assessing and adjusting, as needed, what exists today. Addressing these issues will be critically important for the department to strengthen its homeland security programs and operations. We have made about 1,500 recommendations to DHS to address these issues, which the department has or is working to implement, but more work remains. Eight years after its establishment and 10 years after the September 11, 2001, terrorist attacks, DHS has indeed made significant strides in protecting the nation, but has yet to reach its full potential.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for its review and comment. We received written comments on the draft report from DHS, which are reproduced in full in appendix XIX. DHS also provided technical comments, which we incorporated as appropriate.

DHS acknowledged our work to assess the progress the department has made in enhancing the nation's security and the challenges that still exist. The department discussed its views of its accomplishments since 2001. For example, the department noted its creation and management of the Visa Security Program, which is operational at 19 posts in 15 countries; the increase in the number of deployed Border Patrol agents since 2001; the establishment of fusion centers to serve as focal points for the analysis and sharing of threat and vulnerability-related information; passenger screening and prescreening efforts; and support to state, local, tribal and territorial partners' efforts to enhance emergency communications capabilities, among other things. DHS further noted its issuance of the Quadrennial Homeland Security Review in February 2010, which outlined a strategic framework for homeland security. We recognize the department's progress in these and other areas in the report, as well as discuss existing challenges that will be important for DHS to address moving forward.

The department also stated that the report does not address all of DHS's homeland security-related activities and efforts, and that assessments in each area are not comprehensive because we and the DHS IG have

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00749 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.375

completed varying levels of work in each area. The report notes that the results are based on our work on DHS since it began operations, supplemented with work completed by the DHS IG, with an emphasis on work completed since 2008. We also examined updated information and documentation provided by the department in July and August 2011. As identified in the report, we highlighted our work on key DHS programs and efforts, but neither addressed all products that we and the DHS IG issued related to DHS, nor addressed all of DHS's homeland security-related activities and efforts. In addition, each mission area appendix provides examples of other DHS programs and efforts on which we and the DHS IG have not reported or have completed limited work. Thus, this report was not intended to cover all of DHS's homeland security-related activities and efforts. Further, as discussed in the report, because we and the DHS IG have completed varying degrees of work (in terms of the amount and scope of reviews completed) for each functional area, and because different DHS components and offices provided us with different amounts and types of information, our assessments of DHS's progress in each area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 10 areas.

In addition, DHS provided examples of activities and programs that it stated are not reflected in our report that demonstrate progress DHS made in preparing the nation to respond to threats. These programs include the Western Hemisphere Travel Initiative and increased coordination across the federal government to analyze travel-related data, such as through watchlist centers that provide information regarding potential terrorist travel—the Federal Bureau of Investigation's Terrorist Screening Center, the National Counterterrorism Center, the National Targeting Center, and the Human Smuggling and Trafficking Center. This report discusses progress made and work remaining related to the Western Hemisphere Travel Initiative within the border security area. With regard to the various centers, this report acknowledges the activities of the National Targeting Center, but we did not include it in our assessments of progress because we and the DHS IG have completed limited work on it. The other three centers identified by DHS are not managed by the department. Because this report is focused on DHS-specific programs and efforts on which we have previously reported, supplemented by the work of the DHS IG, this report does not discuss these centers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00750 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.376

This report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-3404, or berrickc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors are listed in appendix XX.

Cathleen A. Berrick

Cathleen A. Berrick
Managing Director, Homeland Security and Justice Issues

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00751 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.377

Appendix I: Department of Homeland Security Functional Mission Areas, Sub-Areas, and Performance Expectations

Table 4 presents the performance expectations and sub-areas we identified for each Department of Homeland Security (DHS) functional mission area.

Table 4: DHS Functional Areas, Sub-Areas, and Performance Expectations

Functional Mission Area: Aviation Security
Sub Area #1: Security Workforce
1a: Ensure the screening of airport workers against terrorist watchlist records
1b: Hire and deploy a federal screening workforce
1c: Develop standards for determining aviation security staffing at airports
1d: Establish standards for training and testing the performance of airport screener staff
1e: Establish a program and requirements to allow eligible airports to use a private screening workforce
1f: Train and deploy federal air marshals on high-risk flights
1g: Establish standards for training flight and cabin crews
1h: Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts
1i: Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action
Sub Area #2: Passenger Prescreening
2a: Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List[a]
2b: Develop and implement an international passenger prescreening process to compare passenger information to terrorist watchlists before aircraft departure
Sub Area #3: Checkpoint Screening
3a: Develop and implement processes and procedures for physically screening passengers at airport checkpoints
3b: Develop and test checkpoint technologies to address vulnerabilities
3c: Deploy checkpoint technologies to address vulnerabilities
3d: Establish a program for armed law enforcement officers traveling by commercial aircraft
3e. Utilize behavioral and appearance indicators to identify persons who pose a risk to aviation security
Sub Area #4: Checked Baggage Screening
4a: Deploy explosive detection systems and explosive trace detection systems to screen checked baggage for explosives
4b: Develop a plan to deploy in-line and other optimal baggage screening systems at airports, as appropriate
4c: Pursue the deployment and use of in-line or other optimal baggage screening systems at airports, as appropriate
Sub Area #5: Air Cargo Security
5a: Develop a plan for air cargo security
5b: Develop and implement procedures to screen domestic and in-bound international air cargo
5c: Develop and implement technologies to screen air cargo

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00752 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.378

Sub Area #6: Security of Airports
6a: Establish standards and procedures for effective airport perimeter security
6b: Establish standards and procedures to effectively control access to secured airport areas
6c: Establish procedures for implementing biometric identifier systems for secured airport areas access control
Sub Area #7: Aviation Security Strategic Planning and Coordination
7a: Develop and implement a strategic and risk-based approach for aviation security functions
7b: Strengthen aviation security through partnerships, coordination and information sharing
Functional Mission Area: Chemical, Biological, Radiological, and Nuclear Threats
Sub Area #1: Assessment
1a: Assess emerging chemical, biological, radiological, and nuclear threats and homeland security vulnerabilities
Sub Area #2: Detection and Mitigation
2a: Coordinate deployment of chemical, biological, radiological, and nuclear detection and other mitigation capabilities
2b: Assess and evaluate chemical, biological, radiological, and nuclear detection capabilities and other countermeasures
Functional Mission Area: Critical Infrastructure Protection—Physical Assets
Sub Area #1: Risk Assessment and Planning
1a: Develop a comprehensive national plan for critical infrastructure protection
1b: Establish and maintain a national database of critical systems and assets
1c: Identify and assess risks to critical infrastructure
Sub Area #2: Protection and Resiliency
2a: Provide and coordinate incident response and recovery planning efforts for critical infrastructure
2b: Support efforts to reduce risks to critical infrastructure
Sub Area #3 Partnerships and Coordination Mechanisms
3a: Improve and enhance public/private information sharing involving attacks and risks
3b: Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector
3c: Develop and enhance national analysis and warning capabilities for critical infrastructure
Functional Mission Area: Surface Transportation Security
Sub Area #1: Risk Assessment and Planning
1a: Develop and adopt a strategic approach for implementing surface transportation security functions
1b: Conduct threat, criticality, and vulnerability assessments of surface transportation assets
Sub Area #2: Standards, Inspections, and Training
2a: Issue standards for securing surface transportation modes
2b: Conduct inspections of surface transportation systems
2c: Develop programs to detect contraband and undeclared passengers entering the United States by rail and for tracking the shipment of security-sensitive materials
2d: Provide surface transportation security training
2e: Train and deploy explosives detection canine teams

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00753 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.379

Sub Area #3: Grants
3a: Administer grant programs for surface transportation security
Sub Area #4: Information Sharing
4a: Share information with stakeholders to enhance surface transportation security
Functional Mission Area: Border Security
Sub Area #1: Inspection of Individuals at Ports of Entry
1a: Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry
1b: Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry
Sub Area #2: Inspection of Cargo and Goods at Ports of Entry while Facilitating Commerce
2a: Develop and implement strategies to detect and interdict illegal flows of cargo, drugs, and other items into and out of the United States while facilitating legitimate commerce
Sub Area #3: Securing the Border between Ports of Entry
3a: Develop and implement programs to detect and identify illegal border crossings between ports of entry
3b: Leverage technology, infrastructure, personnel, and information to secure the border between ports of entry
Sub Area #4: Enhancing Security in the Visa Issuance and Travel Documentation Process
4a: Enhance security measures in the visa issuance process
4b: Enhance the security of certain documents used to enter the United States
Sub Area #5: Collaborating on Border Security Efforts
5a: Enhance collaboration with international, federal, state, local, and tribal law enforcement as well as community groups and the private sector to increase border security, exchange relevant information, and facilitate commerce
Sub Area #6: Border Security Resources
6a: Ensure adequate assets and facilities (at ports of entry for moving people and cargo)
6b: Provide adequate training and equipment for all border-related employees
6c: Develop and implement staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission
Functional Mission Area: Maritime Security
Sub Area #1: Port Facility and Vessel Security
1a: Develop regional (port-specific) plans for security
1b: Develop regional (port-specific) plans for response
1c: Develop regional (port-specific) plans for recovery
1d: Develop, update, and coordinate protocols for resuming trade after a transportation security disruption or incident
1e: Ensure port facilities have completed vulnerability assessments and developed and implemented security plans
1f: Implement a port security grant program to help facilities improve their security capabilities
1g: Implement a national facility access control system for port secured areas
1h: Ensure that vessels have completed vulnerability assessments and developed and implemented security plans
1i: Exercise security, response, and recovery plans with key maritime stakeholders to enhance security, response, and recovery efforts

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00754 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.380

Sub Area #2: Maritime Domain Awareness and Information Sharing
2a: Develop a national plan to establish and improve maritime intelligence
2b: Establish operational centers to monitor threats and fuse intelligence and operations at the regional/port level
2c: Collect and analyze information on incoming vessels to assess risks and threats
2d: Develop and implement a vessel-tracking system to improve intelligence and maritime domain awareness on vessels in U.S. waters
2e: Develop and implement a long-range vessel tracking system to improve maritime domain awareness
2f: Identify and address homeland security needs in the Arctic
2g: Develop and implement an international port security program to assess security at foreign ports
Sub Area #3: International Supply Chain Security
3a: Collect and analyze information on arriving cargo for screening purposes
3b: Develop and implement a system for screening and inspecting cargo for illegal contraband and radiation
3c: Develop and implement a program to work with foreign governments to inspect suspicious cargo before it leaves for U.S. ports
3d: Develop and implement a program to work with the private sector to improve and validate supply chain security
3e: Develop standards for cargo containers to ensure their physical security
Sub Area #4: National Planning
4a: Develop national plans for maritime security
4b: Develop national plans for maritime response
4c: Develop national plans for maritime recovery
Functional Mission Area: Immigration Enforcement
Sub Area #1: Investigations of Immigration Offenses
1a: Develop and implement strategies and programs to enforce immigration laws at the workplace
1b: Develop and implement a comprehensive strategy to interdict and prevent trafficking and smuggling of aliens into the United States
1c: Develop and implement a law enforcement strategy to combat criminal alien gangs in the United States and cross-border criminal activity
Sub Area #2: Investigations of Customs Offenses
2a: Disrupt and dismantle cross-border mechanisms for money laundering and financial crimes
2b: Investigate illegal imports and exports that threaten public safety, including illicit commodities, weapons, and drugs
Sub Area #3: Identification, Detention, and Removal of Aliens Subject to Removal
3a: Develop and implement programs to ensure the timely identification, prioritization, and removal of noncriminal aliens subject to removal from the United States
3b: Develop and implement a program to screen and respond to local law enforcement and community reports of aliens who may be subject to removal from the United States
3c: Ensure the identification, prioritization, and removal of criminal aliens subject to removal from the United States
3d: Assess and prioritize the use of alien detention resources to prevent the release of aliens subject to removal
3e: Develop and implement a program to allow for the secure alternative detention of noncriminal aliens subject to removal

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00755 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.381

Sub Area #4: Management and Training of Immigration Enforcement Human Capital
4a: Develop staffing plans for hiring and allocating human capital resources to fulfill the agency's immigration enforcement mission
4b: Provide training, including foreign language training, and equipment for all immigration enforcement personnel to fulfill the agency's mission
Functional Mission Area: Immigration Services
Sub Area #1: Administration of Immigration Benefits
1a: Institute process and staffing reforms to improve application processes
1b: Eliminate the benefit application backlog and reduce application completion times to 6 months
1c: Implement programs to prevent future backlogs from developing
1d: Establish revised immigration application fees based on a comprehensive fee study
1e: Capture biometric information on all benefits applicants
1f: Implement an automated background check system to track and store all requests for immigration benefits
1g: Establish online access to status information about benefit applications
1h: Establish online filing for benefit applications
1i: Communicate immigration-related information to other relevant agencies
1j: Establish a timetable for reviewing the program rules, business processes, and procedures for immigration benefit applications
1k: Institute a case management system to manage applications and provide management information
Sub Area #2: Immigration Benefit Fraud
2a: Create and maintain an office to reduce immigration benefit fraud
2b: Establish and enhance training programs to reduce fraud in the benefits process
2c: Implement a fraud assessment program to reduce benefit fraud
Sub Area #3: Immigrant Integration
3a: Promote immigrant integration by enhancing understanding of U.S. citizenship and providing support to immigrants through the naturalization process
Functional Mission Area: Critical Infrastructure Protection—Cyber Assets
Sub Area #1: Risk Assessment and Planning
1a: Develop a comprehensive national plan for critical infrastructure protection
1b: Establish and maintain a national database of critical systems and assets
1c: Identify and assess risks to critical infrastructure
Sub Area #2: Protection and Resiliency
2a: Provide and coordinate incident response and recovery planning efforts for critical infrastructure
2b: Support efforts to reduce risks to critical infrastructure
Sub Area #3: Partnerships and Coordination Mechanisms
3a: Improve and enhance public/private information sharing involving attacks and risks
3b: Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector
3c: Develop and enhance national analysis and warning capabilities for critical infrastructure

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00756 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.382

Functional Mission Area: Emergency Preparedness and Response
Sub Area #1: National Emergency Preparedness and Response Planning
1a: Develop a national incident management system
1b: Coordinate implementation of a national incident management system
1c: Establish and implement an all-hazards national response framework
1d: Coordinate implementation of an all-hazards response framework
1e: Develop a complete inventory of federal response capabilities
1f: Develop a national, all-hazards preparedness goal
1g: Develop a national preparedness system
1h: Develop a national preparedness report
1i: Support citizen participation in national preparedness efforts
1j: Develop plans and capabilities to strengthen nationwide recovery efforts
1k: Conduct and support risk assessments and risk management capabilities for emergency preparedness
1l: Establish a comprehensive preparedness assessment system
Sub Area #2: Provision of Emergency Assistance and Services
2a: Develop the capacity to provide needed emergency assistance and services in a timely manner
2b: Provide timely assistance and services to individuals and communities in response to emergency events
2c: Provide oversight of emergency response contracts
Sub Area #3: Emergency and Interoperable Communications
3a: Implement a program to improve interoperable communications among federal, state, and local agencies
3b: Implement procedures and capabilities for effective interoperable communications
3c: Increase the development and adoption of interoperability communications standards
3d: Develop and implement performance goals and measures to assess progress in developing interoperability
3e: Provide grant funding to first responders in developing and implementing interoperable communications capabilities
3f: Provide guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities
3g: Coordinate research, development, and testing efforts to identify and develop technologies to facilitate sharing of emergency alerts and threat-related information
Sub Area #4: Support to State and Local Partners
4a: Provide assistance to state and local governments to develop all-hazards plans and capabilities
4b: Administer a program for providing grants and assistance to state and local governments and first responders
4c: Allocate grants based on assessment factors that account for population, critical infrastructure, and other risk factors
Sub Area #5: Emergency Preparedness Best Practices and Training and Exercise Programs
5a: Develop a system for collecting and disseminating lessons learned, best practices, and threat information to emergency responders and other relevant stakeholders
5b: Establish a comprehensive training program for national preparedness
5c: Establish a program for conducting emergency preparedness exercises

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00757 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.383

Sub Area #6: Emergency Preparedness Human Capital Management
6a: Develop and implement a strategic human capital plan, including filling vacancies and standards for credentialing personnel
6b: Ensure the capacity and readiness of disaster response teams

Source: GAO analysis.

[a] The Selectee and No-Fly lists contain the names of individuals with known or appropriately suspected links to terrorism. These lists are subsets of the federal government's consolidated terrorist watchlist that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00758 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.384

Appendix II: Scope and Methodology

This report addresses the following question: What progress has the Department of Homeland Security (DHS) made in implementing its mission functions since it began operations; w hat work, if any, remains; and what crosscutting and management issues have affected DHS's implementation efforts?

This report is based primarily on work that we have completed since DHS began its operations in March 2003, with an emphasis on reports issued since 2008 to reflect our most recent work, supplemented by DHS Office of Inspector General (IG) reports and updated information and documentation provided by the department in July and August 2011. It is also based on our ongoing work on key DHS programs for various congressional committees, as noted throughout the report. For this ongoing work, we examined program documentation and interviewed agency officials, among other things.

To determine what progress DHS has made in implementing its mission functions and what work, if any, remains, we identified 10 DHS functional areas within its missions, which we define as categories or areas of DHS's homeland security responsibilities. These functional areas are based on those areas we identified for DHS in our August 2007 report on DHS's progress in implementing its mission and management functions, and our analysis of DHS's Quadrennial Homeland Security Review (QHSR) and budget documents, such as its congressional budget justifications.[1] We discussed these functional areas with our subject matter experts and DHS officials and incorporated their feedback as appropriate.[2] These areas include: (1) aviation security; (2) chemical, biological, radiological, and nuclear (CBRN) threats; (3) critical infrastructure protection—physical assets; (4) surface transportation security; (5) border security; (6) maritime security; (7) immigration enforcement; (8) immigration services; (9) critical infrastructure protection—cyber assets; and (10) emergency preparedness and

[1] GAO-07-454.

[2] Our subject matter experts are individuals within GAO who have directed or managed work related to the DHS functional areas.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00759 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.385

response.[3] Within these functional areas, we identified performance expectations, which we define as composites of the responsibilities or functions that the department is to achieve or satisfy based on requirements, responsibilities, and goals set for the department by Congress, the administration, and DHS and its components. In particular, we used expectations identified in our August 2007 report as a baseline, and updated, or added to, these expectations by analyzing:

- Homeland security-related laws enacted since September 2006 to identify legislative requirements for each DHS functional area.[4] Examples of such laws include the Implementing Recommendations of the 9/11 Commission Act of 2007,[5] the Security and Accountability For Every Port Act of 2006 (SAFE Port Act),[6] and the Post-Katrina Emergency Management Reform Act of 2006.[7]
- DHS appropriation acts and accompanying conference reports for fiscal years 2006 through 2011 to identify requirements established and guidance provided to DHS for each functional area.
- Presidential directives and executive orders that have been issued since September 2006 to identify expectations set for DHS by the administration for each functional area. Examples of such directives include Homeland Security Presidential Directive 25: Arctic Region Policy, and Presidential Policy Directive 8: National Preparedness.

[3] We focused these mission areas primarily on DHS's homeland security-related functions. We included U.S. Citizenship and Immigration Services' activities for administering immigration benefits in this report, as they are related to homeland security issues, such as detecting immigration benefit fraud, and are included in the Quadrennial Homeland Security Review. We did not consider the Secret Service, domestic counterterrorism, or intelligence activities because (1) we and the DHS IG have completed limited work in these areas; (2) there are few, if any, requirements we identified for the Secret Service's mission and for DHS's role in domestic counterterrorism and intelligence (the Department of Justice serves as the lead agency for most counterterrorism initiatives); and (3) we address DHS actions that could be considered part of domestic counterterrorism and intelligence in other areas, such as aviation security, critical infrastructure protection, and border security.

[4] We analyzed homeland security-related laws enacted since September 2006 because we had analyzed homeland security-related laws enacted through September 2006 when identifying the expectations we reported in our August 2007 report.

[5] Pub. L. No. 110-53, 121 Stat 266 (2007).

[6] Pub. L. No. 109-347, 120 Stat. 1884 (2006).

[7] Pub. L. No. 109-295, 120 Stat. 1394 (2006).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00760 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.386

- Homeland security-related national strategies that have been issued since September 2006 to identify expectations set for DHS by the administration for each functional area. Examples of such strategies include the 2010 National Security Strategy and 2007 National Strategy for Homeland Security.
- Strategic plans and documents that have been issued since September 2006 by DHS and its component agencies to identify goals and measures established by the department for each functional area. Examples of such strategic plans and documents include the QHSR and Bottom-Up Review (BUR) reports, as well as component level strategic plans, such as the *U.S. Immigration and Customs Enforcement (ICE) Strategic Plan (Fiscal Year 2010-2014)*.

We then grouped the expectations we identified within each functional area into broader sub-areas. Table 5 provides an example of performance expectations and sub-areas for the border security functional area. Appendix I provides the complete list of functional areas, sub-areas, and performance expectations.

Table 5: Example of Performance Expectations and Sub-Areas for Border Security

Functional area	Sub-areas	Performance expectations
Border security	Inspection of individuals at ports of entry	Implement a biometric entry system to prevent unauthorized border crossers from entering the United States through ports of entry
		Implement a biometric exit system to collect information on border crossers leaving the United States through ports of entry
	Inspection of cargo and goods at ports of entry while facilitating commerce	Develop and implement strategies to detect and interdict illegal flows of cargo, drugs, and other items into and out of the United States while facilitating legitimate commerce
	Securing the border between ports of entry	Develop and implement programs to detect and identify illegal border crossings between ports of entry
		Leverage technology, infrastructure, personnel, and information to secure the border between ports of entry
	Border security resources (facilities, assets, and human capital)	Ensure adequate assets and facilities (at ports of entry for moving people and cargo)
		Provide adequate training and equipment for all border-related employees
		Develop and implement staffing plans for hiring and allocating human capital resources to fulfill the agency's border security mission
	Enhancing security in the visa issuance and travel documentation processes	Enhance security measures in the visa issuance process
		Enhance the security of certain documents used to enter the United States

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00761 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.387

Functional area	Sub-areas	Performance expectations
	Collaborating border security efforts	Enhance collaboration with international, federal, state, local, and tribal law enforcement as well as community groups and the private sector to increase border security, exchange relevant information, and facilitate commerce

Source: GAO analysis.

To identify the performance expectations and sub-areas, one analyst independently reviewed the source documents to identify expectations and sub-areas for a functional area. A second analyst then independently reviewed and verified each analysis. We also obtained and incorporated feedback from our subject matter experts on the expectations and sub-areas. In addition, we obtained feedback from DHS and component officials on the expectations and sub-areas we identified, and incorporated their feedback as appropriate.

Further, we then aligned our functional areas to the five Quadrennial Homeland Security Review (QHSR) missions based on our review of the QHSR and BUR reports and DHS's fiscal year 2012 budget documents (see table 6). Within these documents, DHS identified how its initiatives, programs, and activities align or support each QHSR mission, with some supporting more than one mission. For example, U.S. Customs and Border Protection (CBP) identified that its efforts related to inspections at ports of entry and facilitation of trade primarily support QHSR Mission 2: Securing and Managing Our Borders, but also, to a lesser extent, support QHSR Mission 1: Preventing Terrorism and Enhancing Security and Mission 3: Enforcing and Administering Our Immigration Laws. On the basis of DHS's alignment of its initiatives, programs, and activities to QHSR missions, we grouped the 10 functional areas under DHS's QHSR missions. In doing so, we recognized that our functional areas, as well as those key sub-areas that comprise the functional areas, may pertain to more than one QHSR mission area. For example, under our functional area of immigration enforcement, our work addressing the sub-area investigations of immigration offenses addresses DHS programs and activities that relate to more than one QHSR mission—primarily Mission 3: Enforcing and Administering Our Immigration Laws, and also Mission 2: Securing and Managing Our Borders and Mission 1: Preventing Terrorism and Enhancing Security. In those cases when a functional area aligned to more than one QHSR mission, we categorized it under the QHSR mission that it primarily supported on the basis of our review of DHS's QHSR and budget-related documents. In cases when sub-areas within a functional area supported more than one QHSR mission, we kept the sub-area with its functional area (e.g., aviation security) and noted to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00762 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.388

which other QHSR missions it aligned. We provided DHS with our alignment of the functional areas to the QHSR missions, and incorporated the department's feedback, as appropriate.

Table 6: Alignment of Functional Areas under DHS's QHSR Missions

QHSR mission	Functional areas and sub-areas
Mission 1: Preventing Terrorism and Enhancing Security	**Aviation security** • Security of airports • Aviation security workforce • Passenger prescreening • Checkpoint screening • Checked baggage screening • Air cargo security • Aviation security strategic planning and coordination **Chemical, biological, radiological, and nuclear threats** • Assessment • Detection and mitigation **Critical infrastructure protection—physical assets** • Risk assessment and planning • Protection and resiliency • Partnerships and coordination mechanisms **Surface transportation security** • Risk assessment and planning • Security standards, inspections, and training • Grants • Information sharing
Mission 2: Securing and Managing Our Borders	**Border security** • Inspection of individuals at ports of entry • Inspection of cargo and goods at ports of entry while facilitating commerce • Securing the border between land ports of entry • Border security resources • Enhancing security in the visa issuance and travel documentation process • Collaborating on border security efforts • Border security resources **Maritime security** • Port facility and vessel security • Maritime domain awareness and information sharing • International supply chain security • Maritime security national planning

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00763 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.389

QHSR mission	Functional areas and sub-areas
Mission 3: Enforcing and Administering Our Immigration Laws	**Immigration enforcement** • Investigations of immigration offenses • Investigations of customs offenses • Identification, detention, and removal of aliens subject to removal • Management and training of immigration enforcement human capital **Immigration services** • Administration of immigration benefits • Immigration benefit fraud • Immigrant integration
Mission 4: Safeguarding and Securing Cyberspace	**Critical infrastructure protection—cyber assets** • Risk assessment and planning • Protection and resiliency • Partnerships and coordination mechanisms
Mission 5: Ensuring Resilience to Disasters	**Emergency preparedness and response** • National emergency preparedness and response planning • Provision of emergency assistance and services • Emergency and interoperable communications • Support to state and local partners • Emergency preparedness and response best practices and training and exercises programs • Emergency preparedness and response human capital management

Source: GAO analysis of DHS information.

To identify key areas of progress and work that remains in the DHS functional areas, we examined our and the DHS IG's past reports on DHS missions, programs, and operations, including recommendations we and the DHS IG have made, and actions DHS has taken or has underway to address them. We also identified preliminary observations from our ongoing work in some key areas. In doing so, we identified factors that have affected DHS progress in the functional areas. Our work and the work of the DHS IG have covered many of DHS's key programs, operations, and activities. In this report, we highlight our key work in these areas, but do not address all products we or the DHS IG have issued related to DHS, nor did we address all of the sub-areas or DHS's homeland security-related activities and efforts. We selected, in consultation with our subject matter experts, key work we and the DHS IG have completed related to the functional areas and sub-areas. We examined the methodologies used by the DHS IG in its reports, including reviewing the scope, methodological steps, and limitations. We determined that the DHS IG reports were sufficiently reliable for the purposes of our report to provide examples, and to supplement our work,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00764 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.390

of DHS's progress and work remaining. In addition, we obtained data from DHS on its budget authority for fiscal years 2004 through 2011, and funding and staffing levels related to the functional areas, and assessed the reliability of that data by available documentation. We determined that the data were sufficiently reliable for the purposes of our report.

We obtained and incorporated feedback on our assessments within the sub-areas and functional areas from our subject matter experts. In addition, we provided DHS with drafts of our assessments of DHS progress and work remaining in each functional area and obtained and analyzed updated information provided by DHS on these areas. In some cases, DHS provided us with updated data on its efforts, such as statistics on technology deployments or program activities. We assessed the reliability of these data by reviewing available documentation from DHS. We determined that the data were sufficiently reliable for the purposes of our report. We included updated information in our assessments of each sub-area and functional area, based on our review of this information and our prior work. In some cases, we could not make an assessment of the updated information DHS provided because we did not have prior work upon which to base an assessment, or DHS's reported actions were in the early stages of implementation, and thus it was too early to assess the results of these efforts. We noted these instances in our report.

To identify crosscutting and management issues that have affected DHS's implementation efforts, we analyzed the assessments of progress and work that remains in each functional area. We also examined our and the DHS IG's past reports on crosscutting issues, related recommendations, and actions taken by DHS or that are underway to address the recommendations. We obtained and incorporated feedback on the crosscutting issues we identified from our subject matter experts. In addition, we obtained and incorporated feedback from DHS on our assessment of crosscutting issues that have affected the department's mission implementation efforts, including updated information from DHS pertaining to these crosscutting issues. We incorporated updated information into our assessments based on our review of this information and our prior work. In some cases, we could not make an assessment of the updated information DHS provided because we did not have prior work upon which to base an assessment. We noted these instances in our report.

Our assessments of the progress made by DHS in the functional areas and sub-areas, as well as our analyses of crosscutting issues, are based

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00765 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.391

primarily on our issued reports, and supplemented by DHS IG reports. As such, the assessments of progress do not reflect, nor are they intended to reflect, the extent to which DHS's actions have made the nation more secure in each area. Additionally, we do not intend to imply that our discussion of progress and work remaining in the functional areas and sub-areas, considered separately or together, reflect DHS's progress in implementing all of its missions. We also did not assign a qualitative rating of progress for each area. DHS developed other performance measures against which to gauge its progress in fiscal year 2011, but has not yet reported on these measures. As such, the department did not have data available across a consistent baseline against which to assess its progress from fiscal years 2004 through 2011. Therefore, we were not able to assess DHS's progress against a baseline for each functional area and sub-area, and we did not apply a weight to the expectations or sub-areas. We also did not consider DHS component agencies' funding levels or the extent to which funding levels have affected the department's ability to carry out its missions as this was not included in the scope of our prior reviews. Further, we did not consider the extent to which competing priorities; external and internal events, such as departmental reorganizations; and resource demands have affected DHS's progress in each area relative to other areas, although competing priorities, events, and resource demands have affected DHS's progress in specific areas.

In addition, because we and the DHS IG have completed varying degrees of work (in terms of the amount and scope of reviews completed) for each functional area and because different DHS components and offices provided us with different amounts and types of information, our assessments of DHS's progress in each area reflect the information available for our review and analysis and are not necessarily equally comprehensive across all 10 areas. Further, for some sub-areas, we were unable to make an assessment of DHS's progress because we and the DHS IG have not conducted recent work in that area or have conducted limited work. More detailed information on those sub-areas for which we did not make an assessment is included in appendices III through XII.

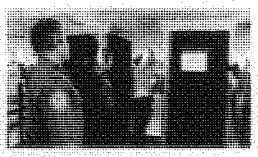
We conducted this performance audit from April 2011 through September 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00766 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.392

Appendix III: Aviation Security

What This Area Includes



Source: TSA.

TSA Employee Demonstrating Use of Advanced Imaging Technology.

The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the lead federal agency responsible for securing all modes of transportation, including aviation. As part of these responsibilities, TSA performs or oversees the performance of security operations at the nation's more than 460 commercial airports.[1] Key elements that comprise aviation security include:

- the aviation security workforce, including hiring, training, and deploying a screening workforce;
- passenger prescreening—comparing passenger information to the Selectee and No Fly lists;[2]
- passenger checkpoint screening, including using staff, policies and procedures, and technology to address potential vulnerabilities;
- checked baggage screening, including deploying explosives detection systems and other technologies to screen baggage for explosives;
- air cargo screening, which involves using staff, policies and procedures, and technology to screen domestic and high-risk international inbound air cargo transported on passenger aircraft; and
- security of airports, including airport perimeter security and access controls.

For fiscal year 2011, TSA had about 54,800 personnel and its budget authority was about $7.7 billion.[3] Aviation security falls primarily within the Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to aviation security also include aviation security

[1] For purposes of this report, the term "commercial airport" refers to a U.S. airport operating under a TSA-approved security program and subject to TSA regulation and oversight. See 49 C.F.R. pt. 1542.

[2] The Selectee and No Fly lists contain the names of individuals with known or appropriately suspected links to terrorism. These lists are subsets of the federal government's consolidated terrorist watchlist that is maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

[3] In addition to TSA, DHS's U.S. Customs and Border Protection plays a role in aviation security by reviewing the passenger and crew manifest of all air carriers destined to the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00767 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.393

strategic planning and coordination, we are not reporting on this area. TSA also relies upon additional programs to deter, detect, and disrupt persons or threats posing a potential risk to aviation security, such as travel document checkers, who examine tickets and forms of identification; random employee screening; intelligence gathering and analysis; random canine team searches at airports; federal air marshals, who provide federal law enforcement presence on selected flights; and reinforced cockpit doors; as well as other measures both visible and invisible to the public. Further, TSA has additional plans and programs related to aviation security, such as TSA's plans to conduct a pilot program on expedited checkpoint screening for low-risk travelers, and TSA's Transportation Systems Integration Facility which supports the development and deployment of new technologies. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that over the past 10 years, TSA has enhanced aviation security in key areas related to the aviation security workforce, passenger prescreening, passenger checkpoint screening, checked baggage screening, air cargo security, and security of airports. For example, TSA hired, trained, and deployed a federal screening workforce. Additionally, after initial difficulty in fielding the program, TSA developed and implemented Secure Flight, a passenger prescreening program through which the federal government now screens all passengers on all domestic and international commercial flights to, from, and within the United States. DHS also developed new programs and is utilizing new technologies to screen passengers and checked baggage, and enhanced the security of domestic and in-bound air cargo. TSA also strengthened security at U.S. airports by assessing risks to airport perimeters and access controls. However, our work has shown that more work remains in these areas. For example, a risk-based strategy and a cost-benefit analysis of airport checkpoint technologies would improve passenger checkpoint screening. Further, TSA does not yet have a procurement plan and schedule for checked baggage screening technologies that would better position TSA to meet recently enhanced explosive detection requirements. Additionally, TSA does not yet have a mechanism to verify the accuracy of domestic and inbound air cargo screening data. Finally, the security of airports would be strengthened by establishing an evaluation plan for pilot tests to screen workers. Table 7 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00768 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.394

Table 7: Assessment of Progress and Work Remaining in Key Aviation Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Aviation security workforce	TSA hired, trained, and deployed a federal screening workforce and other personnel, and deployed programs to enhance in-flight security.	**TSA maintains a federal screening workforce and has deployed programs for in-flight security.** **Key progress:** TSA continues to hire, train, and deploy a federal aviation security workforce. For example, TSA successfully hired, trained, and deployed a federal screening workforce to assume security screening responsibilities at commercial airports nationwide, and developed standards for determining transportation security officer staffing levels at airports. These standards formed the basis of TSA's Staffing Allocation Model, which the agency uses to determine screener staffing levels at airports. In December 2007, we reported that TSA developed a plan that identified the process the agency planned to use to review and validate the staffing model's assumptions on a periodic basis. In July 2011, TSA reported that it was conducting studies on how the staffing model might be adjusted for airport specific environmental factors (e.g., time needed for officers to get to and from off-site training facilities). In addition, TSA has deployed programs and personnel to enhance in-flight security, including training and deploying federal air marshals on high-risk flights, establishing standards for training flight and cabin crews, and establishing a Federal Flight Deck Officer program to select, train, and allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts.
		TSA established explosives detection and other training programs for its screener workforce. **Key progress:** TSA established and continues to deploy numerous programs to train and test the performance of its screening workforce. Among other efforts, TSA provided enhanced explosives-detection training, and reported developing a monthly recurrent (ongoing) training plan for all transportation security officers. In October 2010, the DHS IG reported that, with respect to transportation security officers, the agency lacked standard processes to assign on-the-job training responsibilities. The DHS IG also reported that the agency lacked standard processes to use officer test results to evaluate training program results and evaluate workforce and training needs. The DHS IG recommended that TSA finalize the documentation and implementation of a comprehensive methodology for its transportation security officer training program, and establish and document an on-the-job training program with specific criteria for transportation security officers to serve as on-the-job monitors. TSA concurred with this recommendation and took steps to address it by, for example, updating the draft version of its curriculum development reference guide. In July 2011, TSA reported that it plans to initiate studies to assess the allocation of computers and tools for training.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00769 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.395

Area	Overall assessment	Summary of key progress and work remaining
Passenger prescreening	TSA developed and implemented Secure Flight, a government-operated system that prescreens all passengers traveling to, from, or within the United States.	**TSA prescreens all passengers traveling to, from, or within the United States through its Secure Flight program.** **Key progress:** Passenger prescreening is the matching of airline passenger information against terrorist watchlist records. To conduct this watchlist matching, TSA developed and implemented Secure Flight, a government-operated system that prescreens all passengers traveling to, from, or within the United States. In April 2010, we reported that after initial problems in fielding the program, TSA generally achieved all of the 10 statutory conditions related to the development of the Secure Flight program. The statutory conditions addressed issues such as establishing a process for passengers to correct erroneous information; operational safeguards to reduce opportunities for abuse; and appropriate life-cycle cost estimates.[a] As of June 2010, TSA deployed Secure Flight to cover all domestic and international flights operated by U.S. air carriers, and as of November 2010, to foreign air carriers with commercial flights into, out of, and within the United States.[b] In July 2011, TSA estimated that, on average, Secure Flight prescreens 2 million passenger enplanements per day.[c] TSA also estimated that, on average, Secure Flight identifies more than 200 matches against the No Fly and Selectee lists per month.[d] TSA also reported that it is in the process of implementing Secure Flight reporting for covered flights that fly over U.S. territory to reduce the likelihood of foreign air carriers incurring costly flight diversions resulting from passengers on-board who match the No Fly List.
Passenger checkpoint screening	DHS took steps to enhance passenger checkpoint screening through the implementation of standard operating procedures and the use of advanced imaging technology[e] and behavioral indicators. However, a risk-based strategy, a cost-benefit analysis of technologies, and a comprehensive validation of the science supporting TSA's behavioral analysis program are needed to improve efforts.	**DHS established passenger checkpoint screening standard operating procedures and expanded deployment of advanced imaging technology, but a risk-based strategy and a cost-benefit analysis of technologies would improve efforts.** **Key progress:** Passenger checkpoint screening is comprised of personnel who operate the checkpoint, standard operating procedures that screeners are to follow to conduct screening, and technology used during screening. TSA developed and implemented passenger checkpoint screening standard operating procedures and technologies. In making modifications to passenger checkpoint screening standard operating procedures, TSA considered the daily experiences of airport staff, complaints and concerns raised by the traveling public, and analysis of risks to the aviation system. TSA also made efforts to balance the impact on security, efficiency, and customer service when deciding which modifications to implement. In addition, TSA completed a strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies, and tested and deployed technologies to strengthen checkpoint screening. More recently, in response to the December 25, 2009, attempted attack on Northwest flight 253, TSA revised the advanced imaging technology procurement and deployment strategy, increasing the planned deployment of advanced imaging technology from 878 to between 1,350 and 1,800 units, and using advanced imaging technology as a primary—instead of a secondary—screening measure where feasible.[f] In July 2011, TSA reported that there were 488 advanced imaging technology units deployed at 78 airports throughout the United States.[g] TSA also reported that it is investing in new software for the units to enhance privacy by eliminating passenger-specific images and indicating potential threat items on a generic outline of a person. TSA plans to install this new software on every currently deployed unit in the fall of 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00770 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.396

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We identified work remaining in DHS's efforts to develop and deploy checkpoint technologies. For example, as we reported in October 2009, TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based and did not reflect some of the key risk management principles set forth in DHS's *National Infrastructure Protection Plan*. Specifically, TSA's strategic plan did not reflect the principle of conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and developing a cost-benefit analysis and performance measures.[n] Furthermore, in October 2009, we reported that since the establishment of TSA in November 2001, 10 passenger screening technologies had been in various phases of research, development, test and evaluation, procurement, and deployment, but TSA had not deployed any of these technologies to airports nationwide. Technologies that have now been deployed to airports include advanced imaging technology, advance technology X-ray, and bottle liquid scanners. However, we reported problems with some of these technologies. For example, in March 2010, we reported that it was unclear whether the advanced imaging technology would have detected the weapon used in the December 2009 incident based on the preliminary testing information we received. We have made recommendations to DHS to strengthen its efforts to develop and implement screening technologies at passenger checkpoints. In October 2009, we recommended, among other things, that DHS (1) conduct a risk assessment and develop performance measures for passenger screening technologies, and (2) to the extent feasible, ensure that technologies have completed operational tests and evaluations before they are deployed. DHS concurred with these recommendations and took steps to address them, such as working to develop a Risk Management and Analysis Toolset, to simulate the potential of some technologies to reduce the risk of certain threat scenarios which will apply specifically to the passenger screening process. In addition, we recommended that DHS conduct a cost-benefit analysis of technologies. DHS concurred and reported that it is currently finalizing a cost-benefit analysis for the advance imaging technology, for example. As we reported in March 2010, cost-benefit analyses are important because they help decision makers determine which protective measures, for instance, investments in technologies or in other security programs, will provide the greatest mitigation of risk with available resources. As TSA is in the process of finalizing its cost-benefit analysis, it is too early to assess its results.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00771 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.397

Area	Overall assessment	Summary of key progress and work remaining
		TSA has utilized behavioral indicators to identify persons who pose a risk to aviation security, but TSA has not yet fully validated the science supporting its behavior detection techniques. **Key progress:** As we reported in May 2010, TSA is screening passengers using TSA staff trained in behavior detection principles. TSA deployed about 3,000 Behavior Detection Officers to 161 airports as part of its Screening of Passengers by Observation Techniques program, at an annual cost of over $200 million. If TSA receives its requested appropriation for fiscal year 2012, TSA would be in a position to have invested about $1 billion in the program since fiscal year 2007. In May 2010, we reported that TSA had not validated the science supporting the program or determined if behavior detection techniques could be successfully used across the aviation system to detect threats before deploying the program. We recommended, among other things, that TSA convene an independent panel of experts to review the methodology of a study that the DHS Science and Technology Directorate was conducting on the program to determine whether the study's methodology was sufficiently comprehensive to validate the program. DHS concurred and stated that its validation study, completed in April 2011, included an independent review of the study with input from a broad range of federal agencies and relevant experts, including those from academia. DHS's validation study found that the program was more effective than random screening to varying degrees. However, the study identified that more work was needed to determine whether the science can be used for counterterrorism purposes in the aviation environment. The DHS study made recommendations related to strengthening the program and conducting a more comprehensive validation of the science for use in the aviation environment. TSA is reviewing the study's findings and assessing the steps needed to address DHS's recommendations. **What remains to be done:** Given that DHS's validation study was not designed to fully validate whether behavior detection can be used to reliably identify individuals who pose a security risk in an airport setting, it is not clear whether this program is the most effective use of TSA's resources.
Checked baggage screening	Through its Electronic Baggage Screening Program, TSA developed and deployed systems for screening checked baggage, but needs a plan for updating its explosives detection systems.	**TSA developed and deployed systems to screen checked baggage, but lacks a plan for updating its explosives detection systems.** **Key progress:** TSA's Electronic Baggage Screening Program—which facilitates the development and deployment of optimal checked baggage screening solutions to the nation's airports—is one of the largest acquisition programs in DHS. TSA uses two types of technology for checked baggage screening—the explosives detection system (in both in-line and stand-alone configurations) and the explosives trace detection machine—at the over 460 U.S. commercial airports. Optimal airport solutions may consist of explosives detection systems in either the in-line or stand-alone configuration, or explosives trace detection machines, depending on airport size and other factors. In January 2010, TSA revised explosives detection system requirements to better address current threats and plans to implement these requirements in a phased approach.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00772 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.398

Area	Overall assessment	Summary of key progress and work remaining
		In March 2005, we reported that airports benefit from the installation of more efficient systems, such as in-line baggage screening systems, because these systems reduce the time needed for baggage screening and allow airports and TSA to streamline their operations. We also reported that TSA had not conducted a systematic, prospective analysis to determine at which airports it could enhance efficiencies and security by installing more efficient in-line systems. We recommended that TSA, among other things, identify and prioritize the airports where the benefits of optimizing baggage screening operations by replacing existing baggage screening systems with more efficient in-line systems were likely to exceed the estimated up-front investment costs of installing the systems, or where the systems were needed to address security risks. TSA concurred with this recommendation and published a plan to deploy more efficient systems for 250 airports. In January 2011, TSA reported that it plans to complete its efforts to replace or modify systems at these airports by 2024. In addition, TSA reported in July 2011 that over the next 5 years it intends to shift its focus from completion of optimal airport systems to the replacement of the aging explosives detection systems equipment. TSA is currently working to finalize a recapitalization and optimization strategic plan to prioritize airports' checked baggage screening equipment needs based upon a combination of the age of equipment and maintenance data. We have ongoing work examining, in part, the extent to which TSA has deployed optimal screening systems at commercial airports.' We plan to report on the final results of our work later this year. **What remains to be done:** We identified work remaining in TSA's efforts to screen checked baggage. For example, in July 2011 we reported that TSA faced challenges in procuring the first 260 explosives detection systems to meet TSA's revised 2010 explosives detection systems requirements, which expanded the number and types of explosives that explosives detection systems must detect. Also, TSA had not developed a plan to procure explosives detection systems to meet subsequent phases of the 2010 requirements. In July 2011, we recommended that TSA develop a plan to ensure that new machines, as well as those machines currently deployed in airports, will be operated at the levels in established requirements, and develop a reliable schedule for the Electronic Baggage Screening Program. DHS concurred with these recommendations and has begun taking action to address them, for example, by convening a working group to prepare a plan to procure any additional required technology, and to ensure that a capability gap does not arise from using new explosives detection systems in conjunction with existing explosives trace detection machines. DHS expects to finalize this plan by the fourth quarter of fiscal year 2012. Until TSA develops a plan identifying how it will approach the upgrades for currently deployed explosives detection systems—and the plan includes such items as estimated costs and the number of machines that can be upgraded—it will be difficult for TSA to provide reasonable assurance that its upgrade approach is feasible or cost-effective. Further, while TSA's efforts are positive steps, as TSA does not intend to finalize its plan until fiscal year 2012, it is too early to assess its impact.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00773 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.399

Area	Overall assessment	Summary of key progress and work remaining
Air cargo security	TSA took steps to implement its air cargo security functions, but does not have a data verification mechanism and approved technologies for screening air cargo transported on pallets or in containers.	**TSA took steps to implement its air cargo security functions, but does not have a data verification mechanism and approved technologies for screening air cargo transported on pallets or in containers.** **Key progress:** The Implementing Recommendations of the 9/11 Commission Act of 2007 mandated that DHS establish a system to screen 100 percent of cargo flown on passenger aircraft—including the domestic and inbound flights of foreign and U.S. passenger operations—by August 2010.[j] TSA reported, as of August 2010, that it had established a system to screen 100 percent of domestic air cargo (cargo transported within and outbound from the United States) transported on passenger aircraft in accordance with the mandate. TSA took several actions in meeting this mandate as it applied to domestic cargo, including creating a voluntary program to facilitate screening throughout the air cargo supply chain and taking steps to test technologies for screening air cargo. TSA also took steps to enhance the security of inbound air cargo (cargo bound for the United States), but has not yet fulfilled this portion of the statutory mandate. In January 2011, DHS asked passenger carriers to comment on their ability to screen 100 percent of air cargo on international inbound passenger aircraft by December 31, 2011. As of July 2011, TSA reported that it was reviewing carrier feedback and will use this feedback to help finalize the agency's strategy and timeline for implementing the 100 percent inbound air cargo screening requirement. As part of this effort, TSA reported that the agency will work with industry and foreign government partners to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process, which recognizes foreign government air cargo security programs that TSA determines provide a level of security commensurate with U.S. air cargo security standards. TSA also took steps to enhance the security of inbound air cargo following the October 2010 Yemen air cargo bomb attempt—such as requiring additional screening of high-risk air cargo prior to transport on an all-cargo aircraft. **What remains to be done:** We identified work remaining in TSA's efforts to develop and implement air cargo screening policies and procedures and questioned whether TSA would be able to effectively screen inbound air cargo by the end of 2011, as TSA estimated, given limitations in technology and screening data. In June 2010 we reported that TSA did not have a mechanism to verify the accuracy of domestic and inbound air cargo screening data. Further, there was no technology approved or qualified by TSA to screen cargo once it is loaded onto a unit-load device pallet or container—both of which are common means of transporting air cargo on wide-body passenger aircraft, thus requiring that screening occur before incorporation into pallets and containers. We made a number of recommendations to DHS to strengthen air cargo screening. For example, in June 2010, we recommended that TSA develop a mechanism to verify the accuracy of all screening data, both self-reported domestic and inbound data for cargo transported on passenger aircraft, through random checks or other practical means. TSA partially concurred and has actions underway to address this recommendation, noting that while current screening percentages are based on actual data reported by air carriers, verifying the accuracy of the screening data is difficult. However, TSA is not yet positioned to verify the accuracy of screening data. Verifying industry-reported screening data should better position TSA in providing reasonable assurance that screening is being conducted at reported levels. We are continuing to review these issues and plan to report on our results early next year.[k]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00774 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.400

Area	Overall assessment	Summary of key progress and work remaining
Security of airports	TSA implemented various activities to strengthen security of airports, such as assessing risks to airport perimeters, establishing access controls to secure areas of airports, and expanding requirements for worker background checks. However, an evaluation plan for pilot tests to screen workers would improve these efforts.	**TSA strengthened airport security, such as assessing risks to airport perimeters. However, efforts should be further enhanced by establishing an evaluation plan for pilot tests to screen workers.** **Key progress:** In September 2009, we reported that TSA used several means to identify and assess potential threats to airport security, such as daily intelligence briefings, weekly suspicious incident reports, and situational awareness reports, all of which are available to internal and external stakeholders. TSA also issues an annual threat assessment of the U.S. civil aviation system, which includes an assessment of threats to airport perimeter and access control security. According to TSA officials, these products collectively formed TSA's assessment of threats to airport perimeters and access controls. Additionally, TSA took steps to enhance airport security by expanding its requirements for conducting worker background checks and implementing a random worker screening program. **What remains to be done:** We identified several challenges to strengthening security of airports. For example, we reported in September 2009 that TSA had implemented activities to assess risks to airport perimeters and access controls. We also reported that TSA had conducted joint vulnerability assessments (assessments conducted jointly by TSA and the Federal Bureau of Investigation) at about 13 percent of the approximately 450 commercial airports nationwide, at that time. We also reported, however, that such assessments had not been conducted at 87 percent of the nation's commercial airports and that TSA had not conducted any consequence assessments. As we noted in our 2009 report, TSA officials said that they did not know to what extent the 87 percent of commercial airports, most of which were smaller airports, were vulnerable to an intentional security breach. In July 2011, we reported that joint vulnerability assessments had not been conducted at 83 percent of the nation's airports. In July 2011, TSA told us that plans are being developed to conduct joint vulnerability assessments at more airports as deemed appropriate. Additionally, TSA reported that TSA's national inspection program requires that transportation security inspectors conduct vulnerability assessments at all commercial airports, which are based on the joint vulnerability assessment model. According to TSA, every commercial airport in the United States receives a security assessment every year, including an evaluation of perimeter security and access controls. As we noted in our 2009 report, TSA identified joint vulnerability assessments, along with professional judgment, as the agency's primary mechanism for assessing airport security vulnerabilities in accordance with *National Infrastructure Protection Plan* requirements. We have not yet assessed the extent to which transportation security inspectors consistently conduct vulnerability assessments based on the joint vulnerability model as TSA stated.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00775 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.401

Area	Overall assessment	Summary of key progress and work remaining
		Further, in September 2009, we reported that significant limitations in TSA's design and evaluation of pilot tests to screen airport workers, such as the limited number of participating airports—7 out of about 450, at the time—made it unclear which method was most cost-effective. In addition, we reported that TSA's efforts were not guided by a unifying national strategy that identified key elements, such as goals, priorities, performance measures, and required resources. We made recommendations to TSA to strengthen airport perimeter security and access controls. For example, we recommended in September 2009 that TSA develop a comprehensive risk assessment of airport security and evaluate the need to conduct an assessment of security vulnerabilities at airports nationwide. DHS concurred and said, for example, that it would include an assessment of airport perimeter and access control security risks as part of a comprehensive assessment for the transportation sector, which DHS did in the *Transportation Sector Security Risk Assessment*, published in July 2010. This document included an assessment of various risk-based scenarios related to airport perimeter security but did not consider the potential vulnerabilities of airports to an insider attack—the insider threat—which DHS recognized as a significant issue. In July 2011, TSA officials told us that the agency was developing a framework for insider risk that is to be included in the next iteration of the assessment, which TSA expected to be released at the end of calendar year 2011. Such action, if taken, would meet the intent of our recommendation. We further recommended that DHS ensure that future airport security pilot programs include a well-developed evaluation plan. TSA concurred with this recommendation, and in August 2011 reported that, because it has no current plans to conduct another pilot program, it has not yet taken action to address this recommendation. Additionally, we recommended that TSA develop a national strategy for airport security that incorporates key characteristics of effective security strategies, such as measurable goals and priorities. DHS concurred and stated that it would update its Transportation Systems-Sector Specific Plan to include these characteristics. TSA provided a copy of the updated plan to congressional committees in June 2011 and to us in August 2011. We reviewed this plan and its accompanying aviation model annex and found that while the plan provided a high-level summary of program activities for addressing airport security such as the screening of workers, the extent of which these efforts would be guided by measurable goals and priorities, among other things, was not clear. Providing such additional information would better address the intent of our recommendation.

Source: GAO analysis

Note: This table also includes examples from selected DHS IG reports.

[a] See, e.g., Department of Homeland Security Appropriations Act, 2005, Pub. L. No. 108-334, § 522(a), 118 Stat. 1298, 1319 (2004) (setting forth 10 statutory conditions that DHS must have satisfied before deploying or implementing the passenger prescreening program that is today referred to as Secure Flight).

[b] In addition to TSA's Secure Flight program, CBP also screens passengers on all flights arriving in and departing from and within the U.S. prior to boarding a flight or vessel. This review process starts up to 72 hours prior to departure through scrutiny of airline Passenger Name Records, provided through agreements with the carriers. On the day of departure, when an individual checks in for the intended flight, the basic biographic information from the individual's passport is collected by the air carrier and submitted to CBP.

[c] Enplanements are the number of passengers who board a plane. We did not independently verify the accuracy of these data.

[d] We did not independently verify the accuracy of these data.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00776 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.402

[e] Advanced imaging technology produces an image of a passenger's body that TSA personnel use to look for anomalies, such as explosives and other prohibited items.

[f] Passengers undergo either primary and, if circumstances warrant, secondary screening at passenger checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport, and involves passengers walking through a metal detector and their carry-on items being subjected to X-ray screening. Secondary screening is conducted on selected passengers and involves additional screening of both passengers and their carry-on items.

[g] We did not independently verify the accuracy of these data.

[h] Risk is a function of three elements: (1) threat—the probability that a specific type of attack will be initiated against a particular target/class of targets, (2) vulnerability—the probability that a particular attempted attack will succeed against a particular target or class of targets, and (3) consequence—the expected worst case or worst reasonable adverse impact of a successful attack.

[i] We are conducting our work for the Senate Committee on Commerce, Science, and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and Representative Henry C. Johnson, Jr.

[j] See 49 U.S.C. § 44901(g).

[k] We are conducting our work for the House Committee on Homeland Security, the House Subcommittee on Transportation Security, and the Senate Committee on Homeland Security and Governmental Affairs.

GAO Contact

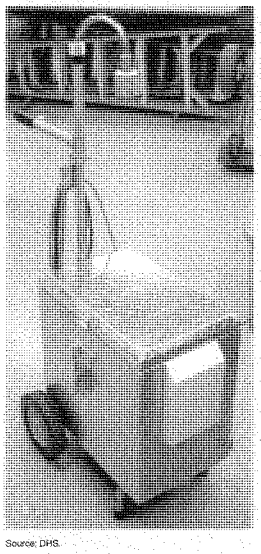
For additional information about this area, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00777 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.403

Appendix IV: Chemical, Biological, Radiological, and Nuclear Threats

What This Area Includes



Source: DHS.
BioWatch Aerosol Collector.

The Department of Homeland Security (DHS) leads federal interagency coordination and planning for emergency response to catastrophic events such as chemical, biological, radiological, and nuclear (CBRN) incidents in the United States, and is responsible for assessing the risks posed by various CBRN agents. These efforts include (1) assessing risks, and (2) developing and deploying capabilities to detect and mitigate CBRN threats. Within DHS, the Science and Technology Directorate (S&T) is responsible for developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for identifying priorities, goals, objectives and policies for, and coordinating the federal government's civilian efforts to identify and develop countermeasures to chemical and biological threats.[1] The Domestic Nuclear Detection Office (DNDO) is responsible for developing, acquiring, and supporting the deployment of a system to detect and report on attempts to develop, transport, or use unauthorized nuclear explosive, fissile, or radiological materials or explosives in the United States. The Office of Health Affairs provides health and medical expertise in support of the DHS mission to prepare for, respond to, and recover from all threats, and leads and coordinates the department's biological and chemical defense activities.

For fiscal year 2011, S&T had about 450 personnel and budget authority of about $830 million. For fiscal year 2011, DNDO had about 130 personnel and budget authority of approximately $340 million. For fiscal year 2011, the Office of Health Affairs had about 95 personnel and budget authority of approximately $140 million. Chemical, biological, radiological, and nuclear threats assessment, detection, and mitigation primarily falls within the Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS has developed and implemented other efforts related to CBRN assessments and detection and mitigation capabilities on which we are not reporting. For example, DHS has initiated efforts related to incidents involving contaminated debris, biodefense exercises and notification procedures for biological attacks. Further, in August 2011 DHS reported to us that it had (1) developed a

[1] 6 U.S.C. § 182(2).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00778 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.404

strategic plan and issued guidance for biological threat prevention and response; (2) established a steering committee for anthrax preparedness and response; and (3) established a program that is developing best practices guidance and decision support tools for federal, state, and local stakeholders for preparedness and response to high consequence chemical incidents. DHS also reported launching a National Nuclear Forensics Expertise Development Program in fiscal year 2008 to enhance academic programs and expertise development opportunities in nuclear forensics. Moreover, DHS reported that it was leading development of a national strategic plan for improving nuclear forensics capabilities in the United States. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work has shown that DHS made progress in assessing risks posed by CBRN threats, developing CBRN detection capabilities, planning for nuclear detection, and conducting radiation detection. However, important efforts related to these areas have not been completed. For example, DHS conducted risk assessments for CBRN agents, but should better coordinate with the Department of Health and Human Services by developing written policies and procedures governing development of the assessments. DHS also developed the BioWatch program, which provides early detection of biological threats. However, the next generation of the system, which is to have additional detection capability, has not yet been operationally deployed. Further, DHS established the National Biosurveillance Integration Center, but the center lacks resources necessary for operations, such as data and personnel from its partner agencies. In August 2011, DHS reported that, among other actions, its Office of Health Affairs had begun to develop a new strategy for the Center. DNDO coordinated the development of a strategic plan for the global nuclear detection architecture—a multidepartment effort to protect against terrorist attacks using nuclear and radiological materials through coordinated activities—and DHS made progress in deploying radiation detection equipment. However, work remains in implementing the global nuclear detection strategy, and DHS faced difficulties in developing new technologies to detect radiological and nuclear materials. For example, DHS's strategic plan for the global nuclear detection architecture addressed some key components of what we previously recommended be included in a strategic plan, such as identifying the roles and responsibilities for meeting strategic objectives. However, the plan did not identify funding needed to achieve the strategic plan's objectives, or employed monitoring mechanisms for determining programmatic progress and identifying needed improvements. Table 8

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00779 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.405

provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 8: Assessment of Progress and Work Remaining in Key CBRN Threats Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
CBRN risk assessments	DHS conducted CBRN risk assessments, but should improve its coordination with agencies by developing procedures for developing the assessments.	**DHS assessed risks posed by CBRN threats, but should strengthen these efforts through improved interagency collaboration by developing written procedures for development of risk assessments.** **Key progress:** The May 2010 National Security Strategy noted that the American people face no greater or more urgent danger than a terrorist attack with a nuclear weapon, as well as the concern that the effective dissemination of a lethal biological agent within a U.S. city would endanger the lives of hundreds of thousands of people and would have unprecedented consequences. Both risk assessment and early detection are elements of assessing the potential for such an attack and its consequences. We reported in June 2011 that DHS develops risk assessments of CBRN threats and had issued seven classified CBRN risk assessments since 2006.[a] We also reported that DHS assessed the threat posed by specific CBRN agents in order to determine which of those agents pose a material threat to the United States, known as material threat assessments. As of June 2011, DHS had conducted 17 material threat assessments, each of which assessed the threat posed by a given CBRN agent or class of agents and the potential numbers of human exposures in plausible, high-consequence scenarios. **What remains to be done:** In June 2011 we reported that although DHS and the Department of Health and Human Services had coordinated with each other and with other federal departments to develop the CBRN risk assessments and material threat assessments, neither department had written procedures or interagency agreements for developing these assessments. In addition, we found that DHS's processes and coordination on the development of such assessments had varied, and reported that Health and Human Services officials stated they would like to be more involved. We recommended that DHS establish time frames and milestones to better ensure timely development and interagency agreement on written procedures for the development of DHS's CBRN risk assessments. DHS concurred and stated that it has begun developing a Strategic Implementation Plan for conducting the assessments. Developing a strategic implementation plan should help DHS better ensure timely development of risk assessments, but since this plan is in development, it is too early to assess its effectiveness.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00780 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.406

Area	Overall assessment	Summary of key progress and work remaining
Development and deployment of CBRN detection and mitigation capabilities	DHS made progress related to the development and deployment of both biological and radiation detection equipment. However, more work remains to enhance collaboration and implement the global nuclear detection architecture.	**DHS made progress in the early detection, warning, and analysis of biological threats through its BioWatch program and the National Biosurveillance Integration Center; however, challenges remain in the clarity of roles and responsibilities related to biosurveillance efforts.** **Key progress:** To detect specific airborne biological threat agents, DHS implemented the BioWatch program, which monitors air samples in more than 30 metropolitan areas and, according to DHS, supports National Special Security Events. The Implementing Recommendations of the 9/11 Commission Act of 2007 established, within DHS, the National Biosurveillance Integration Center, with a mission of, among other things, enhancing the capability of the federal government to rapidly identify, characterize, localize, and track biological events of national concern.[5] The National Biosurveillance Integration Center was to help provide early detection and situational awareness by integrating information and supporting an interagency biosurveillance community. In December 2009, we reported that the Center made efforts to acquire data from its federal partners, obtain analytical expertise from other agencies, establish governance bodies to develop and oversee the community of federal partners, and provide information technologies to support data collection, analysis, and communication. **What remains to be done:** DHS reported that it was developing new detection technology, known as Generation 3.0, beginning in June 2008, which would replace the existing BioWatch technology and would provide a fully automated detector that both collects air samples and analyzes them for threats. In particular, DHS reported that the Generation 3.0 system improves detection times, increases population coverage, and provides greater cost effectiveness. We reported in December 2009 that the National Biosurveillance Integration Center, within DHS's Office of Health Affairs, was not fully equipped to carry out its mission because it lacked key resources, including data and personnel, from its partner agencies, with only 2 of 11 partner agencies having assigned personnel to the Center. In interviews with partner agencies, we found widespread confusion, uncertainty, and skepticism about the value of participation in the Center, as well as the mission and purpose of the Center within its community of federal partners. We noted that for the Center to obtain the resources it needs to meet its mission, it must effectively employ collaborative practices, and we recommended that the Center work with its interagency advisory body to develop a strategy for addressing barriers to collaboration, such as the lack of clear mission, roles, and procedures, and to develop accountability mechanisms to monitor these efforts. DHS concurred and, as of March 2011, reported that it was working to develop a collaboration strategy and performance measures. DHS reported that in August 2010, the Office of Health Affairs had initiated a review of the Center to enhance its ability to identify, characterize, localize, and track biological events of national concern. In addition, DHS is working with the Institute of Medicine to develop a report by the summer 2011 to help inform its strategy and define biosurveillance key terms, such as the mission, roles, and responsibilities. As DHS is working to implement these efforts, it is too early to assess their results.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00781 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.407

Area	Overall assessment	Summary of key progress and work remaining
		DNDO coordinated the development of a strategic plan for the global nuclear detection architecture, but work remains in implementing the global nuclear detection strategy, and DHS faced difficulties in developing new technologies to detect radiological and nuclear materials. **Key progress:** Since December 2010, DNDO has coordinated the development of an interagency strategic plan to guide the development of the global nuclear detection architecture—the overall mission of the architecture is to protect against terrorist attacks using nuclear and radiological materials through coordinated detection, analysis, and reporting of the unauthorized importation, possession, storage, transportation, development, or use of such materials—and an annual report on the current status of the architecture.[c] **What remains to be done:** In July 2011, we testified that DHS's strategic plan addressed some key components of what we previously recommended be included in a strategic plan, such as identifying the roles and responsibilities for meeting strategic objectives. However, we found that neither the plan nor the annual report identified funding needed to achieve the strategic plan's objectives, or employed monitoring mechanisms for determining programmatic progress and identifying needed improvements. DHS officials told us that they will address these missing elements in an implementation plan, which they plan to issue by the end of 2011. As DHS has not yet issued this plan, we could not assess the extent to which it will address the elements we identified. In addition, since 2006 we have reported on difficulties faced by DHS in developing new technologies to detect nuclear and radiological materials. Specifically, we have reported on longstanding problems with DNDO's efforts to deploy advanced spectroscopic portal radiation detection monitors. The spectroscopic portal radiation detection monitors are a more advanced and significantly more expensive type of radiation detection portal monitor to replace the existing polyvinyl toluene portal monitors in many locations that the U.S. Customs and Border Protection (CBP) currently uses to screen cargo at ports of entry. We have issued numerous reports regarding problems with the cost and performance of the advanced spectroscopic portal monitors and the lack of rigor in testing this equipment. For example, we found that tests DNDO conducted in early 2007 used methods that enhanced the apparent performance of advanced spectroscopic portal radiation detection monitors and did not use critical CBP operating procedures that were fundamental to the performance of current radiation detectors. In July 2011, DHS announced that DNDO and CBP would end development of the advanced spectroscopic portal monitors as originally conceived given the challenges the program has faced. However, DNDO reported to us that it plans to deploy 9 of the remaining already procured advanced spectroscopic portal machines at ports of entry, in addition to the 4 already deployed, to gather more complete data about operational needs.

Source: GAO analysis.

[a] DHS issued three bioterrorism risk assessments in 2006, 2008, and 2010; two chemical terrorism risk assessments in 2008 and 2010; and two integrated CBRN terrorism risk assessments in 2008 and 2011. DHS also plans to issue the first radiological and nuclear terrorism risk assessment in 2011.

[b] 6 U.S.C. § 195b.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00782 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.408

[c] The global nuclear detection architecture is a multi-departmental effort coordinated by DNDO, and the strategic plan establishes a broad vision for the architecture, identifies crosscutting issues, defines several objectives, and assigns mission roles and responsibilities to the various federal entities that contribute to the architecture.

GAO Contacts

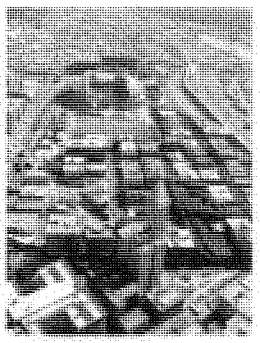
For additional information about this area, contact William O. Jenkins, Jr. at (202) 512-8757 or jenkinswo@gao.gov, or Gene Aloise at 202-512-6870 or aloisee@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00783 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.409

Appendix V: Critical Infrastructure Protection—Physical Assets

What This Area Includes



Source: GAO.
Downtown Seattle and Port Area.

Under the Homeland Security Act of 2002, the Department of Homeland Security (DHS) has wide-ranging responsibility to lead and coordinate the nation's efforts to secure critical infrastructure.[1] DHS's key responsibilities and efforts include (1) risk assessment and planning; (2) protection and resiliency; and (3) partnerships and coordination mechanisms. DHS leads and coordinates the nation's efforts to enhance protection and resiliency for 18 critical infrastructure sectors. Within DHS, three components are charged with lead responsibility over 11 of the 18 sectors.[2] Specifically, within DHS's National Protection and Programs Directorate (NPPD), the Office of Infrastructure Protection is responsible for the chemical; commercial facilities; critical manufacturing; dams; emergency services; and nuclear reactors, materials, and waste sectors. Also within NPPD, the Office of Cybersecurity and Communications is responsible for the communications and information technology sectors, and the Federal Protective Service (FPS) is responsible for the government facilities sector. The Transportation Security Administration (TSA) is responsible for the postal and shipping sector and in turn shares responsibility with the U.S. Coast Guard for the transportation systems sector. As the primary component responsible for critical infrastructure protection via its Office of Infrastructure Protection, for fiscal year 2011 NPPD had about 2,800 personnel and its budget authority was about $2.3 billion.[3] Critical infrastructure protection of physical assets primarily falls within the

[1] Pub. L. No. 107-296, 116 Stat. 2135 (2002). Homeland Security Presidential Directive 7 further defined critical infrastructure protection responsibilities for DHS and those federal agencies responsible for particular critical infrastructure sectors, such as the chemical, commercial facilities, energy, and transportation sectors. The Directive also directed DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.

[2] In addition to DHS, the other federal agencies that serve as sector-specific agencies include the Department of Defense, which is responsible for the defense industrial base sector; the Environmental Protection Agency, which is responsible for the water sector; the Department of Agriculture and the Food and Drug Administration, which are responsible for the food and agriculture sector; and the Department of Interior, which is responsible for the national monuments and icons sector.

[3] The resource amounts provided here encompass resources for all NPPD programming, including programs which do not focus on critical infrastructure protection and resiliency efforts, such as the U.S. Visitor and Immigrant Status Indicator Technology program, which focuses on providing biometric identification services. According to DHS, NPPD's budget authority for fiscal year 2011 included $1.3 billion in appropriated funds and the authority to acquire another $1.1 billion in fees for FPS. These values do not add up to $2.3 billion due to rounding.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00784 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.410

Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS has developed and implemented other efforts related to critical infrastructure protection on which we are not reporting. For example, according to DHS, it is currently developing measures for critical infrastructure protection and resiliency as part of its efforts to develop the National Preparedness Goal and National Preparedness System directed by Presidential Policy Directive 8: National Preparedness. DHS stated that as part of this effort, it is examining the extent to which these measures incorporate crosscutting considerations such as sustainability, durability, and energy efficiency. As these efforts relate to critical infrastructure protection, we have not completed work on them upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the DHS IG's work, has shown that DHS expanded its efforts to conduct risk assessments and planning, provide for protection and resiliency, and implement partnerships and coordination mechanisms for physical critical assets. DHS updated the *National Infrastructure Protection Plan* to include an emphasis on resiliency (the capacity to resist, absorb, or successfully adapt, respond to, or recover from disasters), and an enhanced discussion about DHS risk management. Also, in the *National Infrastructure Protection Plan*, DHS expanded the discussion of its program to prioritize assets and systems for each of the 18 sectors according to their importance, nationally or regionally. Further, DHS took steps to coordinate with critical infrastructure protection stakeholders through information sharing mechanisms such as council meetings. However, our work and that of the DHS IG has shown that key challenges remain in these areas. For example, DHS's state and local partners who are to provide data for the development of annual lists of critical infrastructure assets and systems noted that time and resource constraints can adversely affect the process. Furthermore, DHS has not fully implemented an approach to measure its effectiveness in working with critical asset owners and operators in their efforts to adopt measures to mitigate resiliency gaps identified during various vulnerability assessments. Moreover, the scope of some risk assessments has been limited and assessment results have not been consistently incorporated into planning efforts. In addition, DHS should take additional action to address barriers faced in sharing

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00785 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.411

information about resiliency strategies with critical infrastructure partners. Table 9 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 9: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection—Physical Assets Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Risk assessment and planning	DHS updated the *National Infrastructure Protection Plan* to include an emphasis on resiliency and an expanded discussion on identifying and prioritizing critical infrastructure. DHS components responsible for specific sectors have used risk-based assessments to enhance critical infrastructure planning and protection; however, the scope of some assessments has been limited and assessments' results have not been consistently incorporated into planning efforts.	**DHS made revisions to the *National Infrastructure Protection Plan* to include an emphasis on resiliency.** **Key progress:** In accordance with the Homeland Security Act and in response to Homeland Security Presidential Directive 7, DHS issued, in June 2006, the first *National Infrastructure Protection Plan*, which provided the overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. DHS issued a revised *National Infrastructure Protection Plan* in January 2009 to include updates to critical infrastructure protection planning.[a] In March 2010, we reported that the revised plan incorporated an increased emphasis on resiliency by treating resiliency on an equal footing with protection.[b] DHS also updated the plan's discussion of DHS's overall risk management framework based on stakeholder input and sectors' experiences performing critical infrastructure protection activities, and increased its emphasis on regional planning. Further, DHS made changes regarding how sectors are to measure the performance of their critical infrastructure protection programs. The 2009 plan also included an additional discussion regarding the development of metrics that assess how well programs reduced the risk to the sector. Additionally, according to DHS, beginning in 2011 sectors are expected to report progress against risk-based outcome statements and metrics in the Sector Annual Reports—a progress report called for by Homeland Security Presidential Directive 7. DHS also stated that it plans to collaborate with the sectors to develop a plan for addressing crosscutting opportunities for improvement in critical infrastructure protection and resiliency.
		DHS's efforts to enhance its ability to identify and prioritize critical infrastructure is evolving. **Key progress:** DHS identifies and prioritizes nationally significant critical assets, systems, and networks to determine which of these face the highest risk, establish risk management priorities, and help inform planning and resource decisions. In March 2010 we reported that DHS's update to the *National Infrastructure Protection Plan* provided an expanded discussion about how DHS identifies and prioritizes critical infrastructure. Specifically, in contrast to the 2006 plan, the 2009 plan included a more detailed discussion of the national critical infrastructure prioritization program that places critical infrastructure into categories according to their importance, nationally or regionally.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00786 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.412

Area	Overall assessment	Summary of key progress and work remaining
		Further, in June 2009, the DHS IG reported that DHS had worked with state homeland security partners to compile annual lists of critical assets and systems and had begun to use consequence-based criteria focused on assets and systems whose disruption could have either catastrophic national consequences or nationally significant consequences. The DHS IG reported that the creation of these lists was complex and difficult for several state partners. For example, the DHS IG reported that (1) some DHS partners noted that time and resource constraints can adversely affect their ability to participate in the data compilation process, and (2) the strength of state critical infrastructure programs varied across the nation, impeding some partners' ability to provide timely and comprehensive information. The DHS IG recommended ways that DHS should enhance partner participation in the list development process and obtain additional resources to enhance asset and system identification efforts. DHS generally concurred and addressed the recommendations. According to DHS, it addressed these recommendations through actions such as developing unclassified lists to provide state level homeland security officials access to information about infrastructure assets and systems critical to their jurisdictions, and leading a national critical infrastructure prioritization program working group to discuss program enhancements with sector partners. Later this year, we plan to begin work for the Senate Committee on Homeland Security and Governmental Affairs; House Committee on Homeland Security and the House Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies examining recent DHS efforts to identify and prioritize critical infrastructure.
		DHS components responsible for specific sectors have begun to use risk-based assessments in critical infrastructure planning and protection, but face challenges in conducting these assessments and should enhance incorporation of their results into planning. **Key progress:** DHS components with responsibility for critical infrastructure sectors have begun to use risk-based assessments in their critical infrastructure related planning and protection efforts, but they have faced implementation challenges. For example, in April 2010, we reported that the Coast Guard used its Maritime Security Risk Analysis Model to help concentrate maritime security activities when and where relative risk is believed to be the greatest. The Model is used to assess the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios—such as the risk to ferries associated with a suicide bomber or a boat attack—consistent with the risk management framework established in the *National Infrastructure Protection Plan*. Also, according to the Coast Guard, the Maritime Security Risk Analysis Model is designed to support national decision making and long term strategic planning, evaluate capabilities needed to combat future terrorist threats, and identify the highest-risk scenarios and targets in the maritime domain. Further, we reported in March 2009 that TSA took action to implement a risk management framework across the surface transportation sector. We issued a series of reports on surface transportation security that found, among other things, that TSA had issued modal strategies intended to guide its efforts to secure the various surface transportation modes. Further, according to TSA, in 2010, it developed risk assessments for highway infrastructure and the trucking and the school bus industries, among others, that were incorporated into the *Transportation Sector Security Risk Assessment*.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00787 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.413

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We have identified weaknesses in DHS components' efforts to implement risk-based assessments in enhancing critical infrastructure planning and protection. For example, we reported that TSA's efforts to conduct threat, vulnerability, and consequence assessments within the individual surface transportation modes had limitations. In April 2009, we reported that TSA's efforts to assess risk to freight rail had primarily focused on one key threat (rail shipments of certain highly toxic materials), although other federal and industry assessments had identified additional potential security threats, including risks to critical infrastructure. In addition, in January 2009, we reported that TSA's strategy for securing the highway mode was not based on completed risk assessments. For example, while nearly all of TSA's and the Office of Infrastructure Protection's available vulnerability assessments were conducted prior to the issuance of the highway security strategy, their results were not used to develop the strategy. We recommended, among other things, that TSA conduct risk assessments that combined threat, vulnerability, and consequence to help produce a comparative assessment within the transportation modes and across the transportation sector—a tool that could also be used for current and future investment decisions. TSA concurred, and in June 2010 TSA produced the *Transportation Sector Security Risk Assessment*, which assessed risk within and across the various transportation modes. TSA expects to complete an enhanced version of the risk assessment at the end of calendar year 2011 to help address limitations it identified in the 2010 assessment.[c] Thus, it is too early to assess the effectiveness of this assessment. In July 2011, TSA also reported developing a methodology for the identification and assessment of critical freight rail infrastructure, such as bridges and tunnels, which includes factors that account for vulnerability and consequence. TSA stated that it uses the results of these assessments to prioritize both railroad infrastructure hardening projects and grants. Further, DHS provided its updated transportation security strategy to congressional committees in June 2011 and to us in August 2011. However, we have not yet assessed the extent to which it addresses our recommendations, as the strategy was recently issued. In addition, we identified challenges that FPS faces in implementing a risk-based staffing plan for protecting federal facilities. For example, in 2009 we reported that, among other things, FPS's workforce planning was limited because FPS headquarters did not collect data on its workforce's knowledge, skills, and abilities. Without such information, we reported that FPS was not able to determine what its optimal staffing levels should be or identify gaps in its workforce needs, and determine how to modify its workforce planning strategies to fill these gaps. FPS drafted a staffing plan in June 2010, consistent with our recommendation. According to FPS, the agency is working to finalize its staffing plan, which has been approved by the Secretary of Homeland Security and provided to the Office of Management and Budget before being submitted to the Secretary of Homeland Security for final approval. As this staffing plan has not yet been finalized, it is too soon to assess its results. Such a plan is needed to help FPS determine what its optimal staffing levels should be, to identify gaps in its workforce needs, and to determine how to modify its workforce planning strategies to fill these gaps.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00788 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.414

Area	Overall assessment	Summary of key progress and work remaining
Protection and resiliency	DHS's efforts to assess protection and resiliency are evolving and include actions to bring a stronger focus to resiliency. However, performance measures are needed to determine the extent to which actions are being taken to address resiliency gaps.	**DHS's efforts to assess protection and resiliency are evolving, but performance measurement should be strengthened.** **Key progress:** DHS has various voluntary programs in place to conduct vulnerability assessments and security surveys at and across facilities from the 18 sectors, and uses these assessments to develop and disseminate information on steps asset owners and operators can take to protect their facilities. In September 2010, we reported that consistent with the updated *National Infrastructure Protection Plan*, DHS had taken action to develop or enhance the programs it uses to work with asset owners and operators to bring a stronger focus to resiliency. For example, in 2009 DHS developed the Regional Resiliency Assessment Program to assess vulnerability, threats, and potential consequences associated with groups of related infrastructure, regions, and systems in major metropolitan areas. The program is intended to identify dependencies, interdependencies, cascading effects, resiliency characteristics, and gaps, and to provide training and other assistance. DHS was also revising assessment tools used to assess vulnerabilities at individual facilities. **What remains to be done:** In September 2010 we reported that DHS had not developed an approach to measure its effectiveness in working with asset owners and operators in their efforts to adopt measures to mitigate resiliency gaps identified during the various vulnerability assessments. We recommended that DHS develop performance measures to assess the extent to which asset owners and operators are taking actions to resolve resiliency gaps identified during these assessments. DHS agreed and has reported that it is taking actions to address the recommendation. According to DHS, these actions include developing performance measures related to the impact of Office of Infrastructure Protection assessments on improving the protection and resilience of critical infrastructure. They also include the development of a mechanism to assess the extent to which asset owners and operators are taking actions to enhance security and resilience with associated output metrics. We are currently conducting a review for the House Committee on Homeland Security assessing DHS's efforts to manage its vulnerability assessment programs, including its efforts to measure the actions owners and operators take to mitigate vulnerabilities identified by DHS. We plan to report on our results in 2012.
		DHS's Protective Security Advisor Program is intended to assist asset owners and operators on protection and resiliency issues. **Key progress:** DHS deployed 93 critical infrastructure protection and security specialists, called Protective Security Advisors, to local communities throughout the country to assist asset owners and operators in all 18 sectors on critical infrastructure protection strategies. In September 2010, we reported that DHS had begun to train the Protective Security Advisors about resiliency and how it applies to the owners and operators they interact with. However, we reported that DHS had not updated guidance that outlines the Protective Security Advisors' roles and responsibilities to reflect DHS's growing emphasis on resiliency. We recommended that DHS update the Protective Security Advisor guidance that discusses the role the Security Advisors play during interactions with asset owners and operators with regard to resiliency. DHS agreed and provided additional training and updated guidance to Protective Security Advisors on their role with regard to resiliency during their interactions with owners and operators.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00789 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.415

Area	Overall assessment	Summary of key progress and work remaining
Partnerships and coordination mechanism	DHS took steps to coordinate with critical infrastructure stakeholders to address overlaps and gaps by clarifying roles and responsibilities for agencies that have regulatory oversight for critical infrastructure sectors. However, limited collaboration has hindered federal emergency communication efforts. In addition, DHS shares the results of vulnerability assessments with critical infrastructure partners, but has not developed an approach to disseminate information on resiliency practices within and across sectors.	**DHS took steps to coordinate with critical infrastructure stakeholders to identify security gaps and overlaps, but limited collaboration has hindered federal emergency communication efforts.** **Key progress:** In May 2011, we reviewed the coordination activities of nine critical infrastructure sectors to identify any security overlaps and gaps. While our findings are not generalizable to all 18 sectors, we found that DHS coordinated with critical infrastructure stakeholders, including other federal regulatory authorities, through information-sharing mechanisms, such as council meetings, to identify overlaps and gaps in critical infrastructure security activities. In addition, DHS took action to address overlapping security activities by clarifying roles and responsibilities for critical infrastructure security activities with agencies that have regulatory oversight through coordination mechanisms, including memorandums of understanding and working groups. Furthermore, DHS developed and distributed tools, such as guides, to critical infrastructure sectors and conducted voluntary training and exercises to enhance security capabilities. DHS also conducted vulnerability assessments and security surveys at both public and privately owned facilities that volunteer for such efforts. We are beginning work for the House Committee on Homeland Security on DHS's voluntary programs and its efforts to measure the effectiveness of its voluntary programs in enhancing critical infrastructure protection and resiliency. We plan to report on our efforts in 2012. **What remains to be done:** We also reported on challenges that DHS faces in coordinating with federal partners. For example, in June 2009, we reported that, with respect to the communications sector, limited collaboration and monitoring by DHS and its federal partners hindered federal emergency communications efforts. Federal agencies had demonstrated limited use of some best practices that we previously reported as helpful for addressing issues like emergency communications, such as promoting a public safety network for emergency communications. We recommended, among other things, that DHS and its partners systematically track, assess, and respond to stakeholder groups' recommendations, including identifying opportunities to work with other agencies, as appropriate, to advance recommendations. DHS generally concurred with our recommendations and in response reported that it has taken steps toward addressing them, such as sharing the stakeholder groups' recommendations with the Emergency Communications Preparedness Center, a focal point and clearinghouse for implementing federal interoperable communications efforts. While these are positive steps, it is unclear how the Center would incorporate the work of stakeholder groups. Improved monitoring and accountability of stakeholder and advisory committee's recommendations would boost the value of these groups by monitoring agency responses, avoiding duplication of efforts, and identifying opportunities to work with other agencies.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00790 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.416

Area	Overall assessment	Summary of key progress and work remaining
		DHS shares the results of vulnerability assessments with critical infrastructure partners, but has not developed an approach to disseminate information on resiliency practices within and across sectors. **Key progress:** DHS shares information on potential protective measures with various partners, such as asset owners and operators, and others including state and local officials (generally on a case-by-case basis) after it has completed vulnerability assessments at critical infrastructure facilities. Further, in September 2010 we reported that DHS relies on its private-sector partners to develop and share information on practices they use to enhance their protection and resilience. DHS officials said that the practices shared by sector partners, including best practices, were largely identified and developed by the private sector, at times with the support of its partners in government such as the sector-specific agencies. DHS facilitated this process by making various mechanisms available for information sharing, including information they deemed to be best practices. For example, according to senior DHS officials, DHS's Homeland Security Information Network-Critical Sectors was designed to provide each sector a portal to post useful or important information, such as activities or concepts that private-sector partners discern to be best practices on protection and resiliency topics. **What remains to be done:** DHS faces barriers to sharing information about resiliency strategies. For example, given the voluntary nature of the critical infrastructure partnership, DHS officials stated that DHS should not be viewed as identifying and promoting practices that could be construed by critical infrastructure partners to be standards. Also, according to DHS officials, the need for and the emphasis on resiliency can vary across different types of facilities depending on the nature of the facility. In our September 2010 report, we recognized that DHS faces barriers to information sharing. However, we concluded that as the primary federal agency responsible for coordinating and enhancing the protection and resiliency of critical infrastructure across the sectors, DHS is uniquely positioned to disseminate information on resiliency practices to help asset owners and operators consider and adopt resiliency strategies. Thus, we recommended, among other things, that DHS determine the feasibility of overcoming these barriers and developing an approach to disseminate resiliency information. DHS did not agree with the recommendation, but stated that it would expand the distribution of resiliency products to critical infrastructure stakeholders. In July 2011 DHS reported taking steps to address our recommendation, including disseminating documents related to protection and resiliency that cover some resiliency measures. DHS further reported that as its understanding of stakeholder needs in this area grows, it will be able to synthesize more focused resiliency products. These efforts should better position DHS for sharing resiliency information. However, as our work has shown, DHS needs to determine the feasibility of developing an approach to better disseminate resiliency practices to better position itself to help asset owners and operators consider and adopt resiliency strategies, and provide them with information on potential security investments.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00791 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.417

[e] Our assessment of the two plans was limited to determining how the 2009 *National Infrastructure Protection Plan* changed compared to the 2006 plan, and how DHS and the sectors addressed resiliency as part of their planning efforts.

[f] TSA noted limitations in the June 2010 *Transportation Sector Security Risk Assessment* report that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. For example, the Risk Assessment excluded certain types of threats, such as from lone wolf operators. According to TSA, these limitations will be addressed in the 2011 version.

GAO Contacts

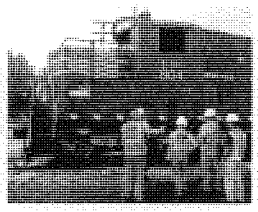
For additional information about this area, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov for overall critical infrastructure protection, or Mark Goldstein at (202) 512-2834 or goldsteinm@gao.gov for government facilities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00792 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.418

Appendix VI: Surface Transportation Security

What This Area Includes



Source: TSA.

TSA Rail Security.

The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the lead federal agency responsible for overseeing security of all surface transportation modes, which include passenger and freight rail; mass transit; highways, including commercial vehicles; and pipelines. Although TSA has primary responsibility for overseeing surface transportation security, this responsibility is shared with federal, state, and local governments and the private sector. For example, public and private operators are responsible for securing their transportation systems. Key areas within surface transportation security include: (1) risk assessment and planning; (2) standards, inspections, and training; (3) grants; and (4) information sharing. As the primary component responsible for surface transportation security, for fiscal year 2011, TSA had about 54,800 personnel and its budget authority was about $7.7 billion for fiscal year 2011, most of which is devoted to aviation security functions. Surface transportation security falls primarily within the Quadrennial Homeland Security Review Mission 1: Preventing Terrorism and Enhancing Security.

For the purposes of this report, we are generally focusing on key areas on which we or the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS developed and implemented additional efforts related to surface transportation security on which we are not reporting. These include, among other things, the Surface Transportation Security Priority Assessment—a public-private study which identified recommendations to enhance surface transportation security; the National Explosives Detection Canine Program; the Baseline Assessment for Security Enhancement—a security assessment program designed to evaluate 17 security and emergency management action items for mass transit and passenger rail networks; a training program in Pueblo, Colorado for highway surface transportation inspectors; the Intermodal Security Training and Exercise Program, which is a training and exercise program for the transportation industry developed by TSA, in collaboration with other federal agencies and commercial security vendors; and standard processes for law enforcement to identify and report suspicious incidents or activities throughout the Amtrak rail system and share that information nationally so it can be analyzed to identify broader trends. We have not completed work in these areas upon which to make an assessment of DHS's progress.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00793 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.419

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS, particularly TSA, expanded its efforts in key areas on which we have reported, such as risk assessments and strategic planning; surface transportation inspector workforce; grants administration; and information sharing. For example, in 2009 we reported that TSA had begun conducting threat and vulnerability assessments of the commercial vehicle industry and that TSA and other DHS agencies conducted threat, vulnerability, and consequence assessments of highway infrastructure, freight rail, and mass transit. TSA also developed a transportation sector security risk assessment that assessed risk within and across the various transportation modes. In addition, since 2008, TSA more than doubled its surface transportation inspector workforce and reported that, as of July 2011, its surface inspectors conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, among other things. Moreover, we reported in June 2009 that DHS used a risk analysis model to allocate Transit Security Grant Program funding and award grants to higher-risk transit agencies. Further, TSA expanded its sharing of surface transportation security information by establishing information networks.

However, we have identified work remaining in these areas. For example, TSA has strengthened its risk assessments for surface transportation modes, but efforts to further improve elements of these assessments are in the early stages of implementation. Further, TSA has not yet completed an analysis of its surface inspector workforce to direct current and future program needs. Moreover, TSA has not issued regulations for security training programs for mass transit, rail, and bus employees, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[1] Additionally, we found that TSA should strengthen the management of its program for providing grant funds to transit agencies, and that its information sharing efforts would benefit from improved streamlining and coordination. Table 10 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

[1] 6 U.S.C. §§ 1137, 1167, 1184.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00794 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.420

Table 10: Assessment of Progress and Work Remaining in Key Surface Transportation Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Risk assessment and planning	DHS employed a strategic approach, including developing national strategies and conducting risk assessments, for each mode of surface transportation, but had not yet developed performance measures for assessing programs' effectiveness.	**DHS developed national strategies for each mode of surface transportation, but had not yet developed measures for assessing progress made in securing surface transportation modes.** **Key progress:** DHS has taken steps to develop and adopt a strategic approach for implementing surface transportation security functions, such as developing national strategies for each surface transportation mode. For example, we reported in June 2009 that TSA's mass transit security strategy contained information related to purpose, scope, and methodology; organizational roles, responsibilities, and coordination; and implementation of the strategy and integration with other strategies. We reported in April 2009 that TSA's freight rail security strategy contained sectorwide goals, subordinate objectives, and performance measures. **What remains to be done:** We identified work remaining in DHS's strategic approaches to security within the different modes of surface transportation. For example, in January 2009, we reported that TSA's highway strategy did not include performance goals and measures with which to assess the program's overall progress toward securing highway infrastructure. In June 2009, we reported that TSA's mass transit security strategy identified sectorwide goals, but did not contain measures or targets for program effectiveness. In August 2010, we reported that TSA's pipeline security strategy identified goals and objectives, but did not include performance measures or milestones. Also, in April 2009, we reported that TSA's freight rail security strategy could be strengthened by including targets for three of its four performance measures and revising its approach for the other measure, such as including more reliable baseline data to improve consistency in quantifying results. We recommended that TSA strengthen its performance measures in its strategies by, for example, measuring the agency's performance in achieving the goals of preventing and deterring acts of terrorism and enhancing the resiliency of mass transit systems. DHS concurred with our recommendations and reported that it was incorporating a risk-based approach with measurable baselines in its updated highway strategy, and revising its mass transit security strategy to incorporate elements to improve its ability to measure agency and industry progress toward achieving mass transit and passenger rail security performance goals. DHS provided its updated transportation security strategy to congressional committees in June 2011 and to us in August 2011. As the strategy was recently issued, we have not yet assessed the extent to which it addresses our recommendations.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00795 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.421

TSA conducted risk assessments within and across the transportation sector, but efforts to strengthen these assessments in certain areas are in the early stages of implementation.

Key progress: TSA conducted risk assessments across the transportation sector and for individual transportation modes. In March 2009, we reported that TSA implemented certain aspects of the *National Infrastructure Protection Plan's* risk management framework, such as developing security goals and a database to track assets and systems. In February 2009, we reported that TSA began conducting threat and vulnerability assessments of the commercial vehicle industry. In January, April, and June 2009, we reported that TSA and other DHS agencies took actions to conduct threat, vulnerability, and consequence assessments of highway infrastructure, freight rail, and mass transit and passenger rail, respectively. Further, in August 2010, we reported that TSA developed a pipeline risk assessment model that combined threat, vulnerability, and consequence to create a risk score for each of the 100 most critical pipeline systems in the United States.

What remains to be done: We identified weaknesses in DHS's risk assessments, which TSA has worked to address. For example, we reported in March 2009 that TSA had not conducted comprehensive risk assessments that integrate threat, vulnerability, and consequence for each mode or the transportation sector. We also reported that TSA should strengthen its internal controls to help implement the *National Infrastructure Protection Plan*'s risk management framework, and that TSA did not assign uncertainty or confidence levels to the intelligence information the agency used to identify threats and guide long-range planning and strategic investment. Additionally, in January 2009 we reported that federal entities—including component agencies and offices within DHS and the Department of Transportation—were not systematically coordinating their efforts to assess highway infrastructure risk or sharing the results of those efforts. In April 2009, we reported that TSA's efforts to assess risk to freight rail primarily focused on rail shipments of certain highly toxic materials, although other federal and industry assessments had identified additional potential security threats, including risks to bridges and tunnels. Additionally, as we reported in August 2010, a pipeline system's risk ranking was not TSA's primary consideration in scheduling Corporate Security Reviews—assessments of pipeline operators' security planning—of pipeline operators or Critical Facility Inspections of pipeline systems.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00796 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.422

		We recommended strengthening risk assessments across surface transportation modes. DHS generally concurred and in June 2010 TSA produced the Transportation Sector Security Risk Assessment, which assessed risk within and across the various aviation and surface transportation modes, and incorporated threat, vulnerability, and consequence. However, TSA noted limitations—such as the exclusion of threats from lone wolf operators—that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. In June 2011, agency officials stated that TSA is addressing these limitations in the next version, which is scheduled for completion by the end of 2011. TSA also established an Executive Risk Steering Committee, which, according to TSA officials, serves as a focal point for strategic risk management. Further, in February 2010, TSA officials stated that the agency had met with other federal agencies that conduct security reviews of highway structures to identify existing data resources, establish a data-sharing system among key agencies, and discuss standards for future assessments. In July 2011, TSA further reported that in 2010 it worked with federal partners to conduct comprehensive structural security assessments of 30 highway structures, such as bridges, tunnels, and terminals. This effort is still in the early stages, with the first report of results under review by TSA and its federal partners. In August 2011, TSA officials stated that the first report for highway bridge and tunnel assessments is expected to be complete before the end of calendar year 2011, and with more to be concluded for presentation to stakeholders by the end of calendar year 2012. As DHS has not yet reported on these assessments, it is too early to review their results. Moreover, TSA is developing a Critical Infrastructure Risk Tool to measure the criticality and vulnerability of freight railroad bridges and tunnels. As of July 2011, TSA officials stated that they had begun working with industry officials to raise awareness of cyber risks to the rail system, although TSA has not conducted assessments of those risks. In addition, in June 2011, TSA reported that it had revised its Corporate Security Review Program's standard operating procedure to identify that the primary selection criterion for scheduling Corporate Security Reviews will be the measure of relative risk, although other factors and considerations will also play a role. While these are positive actions, as TSA is in the process of implementing them, it is too early to assess their effectiveness.
Standards, inspections, and training	DHS more than doubled its surface transportation inspector workforce, but has not issued regulations for security training programs for some surface transportation employees.	**TSA deployed an inspector workforce for surface transportation security, but has not issued regulations for security training programs for mass transit, rail, and bus employees.** **Key progress:** We reported in April 2010 that since 2008 TSA more than doubled its surface transportation inspector workforce, and expanded the roles and responsibilities of surface inspectors to include participation in Visible Intermodal Prevention and Response teams, among other things.[a] TSA reported that, as of July 2011, TSA's surface inspectors conducted security assessments of 193 mass transit and passenger rail agencies, and had conducted over 1,300 site visits to mass transit and passenger rail stations to complete station profiles, which gather detailed information on a station's physical security elements, geography, and emergency points of contact.[b]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00797 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.423

What remains to be done: In June 2009, we reported that TSA had not completed an analysis of its surface transportation inspector workforce to direct current and future program needs. In March 2010, TSA completed a workforce study that was designed to provide the agency with a more reasonable basis for determining the optimal workforce size needed to achieve its current and future inspector workload needs. However, TSA's workforce study was not specific to surface transportation security inspectors, and we have not assessed the extent to which the results of this study are informing TSA's resource allocation decisions. In addition, the authors of the study suggested using their report as a first step toward further study and a more comprehensive and well-coordinated TSA-wide plan of action. TSA also developed a detailed work plan for inspectors—including surface inspectors—for fiscal year 2011. However, neither the work plan nor the workforce study addresses future hiring and training needs for the surface inspector workforce. In August 2011, TSA officials stated that it would be difficult to make such long-term plans until certain key surface transportation rules have been finalized, such as those for security training discussed in the next section, because these rules will directly affect the surface transportation inspector workload.

Additionally, we identified gaps in DHS's efforts to implement surface transportation security training requirements. In June 2009, we reported that TSA had not issued regulations for a training program for mass transit, rail, and bus employees, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007.[c] We recommended that DHS develop a plan with milestones for implementing provisions of the Act. DHS concurred and in June 2011 stated that it had developed a timeline for completing requirements of the Act, to include issuing the training regulations. TSA reported in July 2011 that it is finalizing the proposed security training program regulations and expects to issue a Notice of Proposed Rulemaking for public comment by January 2012.[d] As DHS is in the process of developing these security training program regulations, it is too soon to assess the extent to their effectiveness. As we reported, the implementation of these regulations will be part of a fundamental shift in approach for TSA as it assumes more of a regulatory role in securing mass transit and passenger rail.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00798 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.424

Grants	DHS allocates transit grant funding based on risk assessments and has taken steps to measure performance of the Transit Security Grant Program.[8] However, TSA should further strengthen its management of the grant program.	**DHS implemented the Transit Security Grant Program and uses risk assessments to allocate transit grant funds, but should further strengthen its grants management.** **Key progress:** In fiscal year 2011, DHS made available over $200 million for the Transit Security Grant Program, almost $20 million for intercity rail security, $10 million for freight rail security, and nearly $5 million for intercity bus security. We reported in June 2009 that DHS used a risk analysis model to allocate Transit Security Grant Program funding and award grants to higher-risk transit agencies. The Transit Security Grant Program risk model includes all three elements of risk—threat, vulnerability, and consequence. In addition, DHS developed measures to assess the effectiveness of its grant programs. For example, as the DHS IG reported in December 2010, the Federal Emergency Management Agency (FEMA), in its May 2009 Recovery Act Plan for the Transit Security Grant Program, identified five key performance indicators that it would use to measure the effectiveness of grant performance. Since then, FEMA, working in collaboration with TSA, identified nine additional performance measures for use in conjunction with the measures identified in the May 2009 report. Additionally, TSA reported that it is working with FEMA to develop more robust performance measures to track Transit Security Grant Program management and effectiveness results. FEMA plans to incorporate these performance measures into its fiscal year 2012 grant guidance. In July 2011, TSA also reported a new approach for the Transit Security Grant Program, which focuses resources on the highest risk "shovel ready" transit infrastructure projects, while prioritizing operational deterrence activities such as training and canine teams. **What remains to be done:** We and the DHS IG identified weaknesses in DHS's Transit Security Grant Program, which DHS has worked to address. For example, as we reported in June 2009, in DHS's risk assessments, DHS held vulnerability constant, which limited the model's overall ability to assess risk and DHS's ability to more precisely allocate funds. Moreover, the DHS IG reported in December 2010 that, while DHS developed new performance measures to evaluate the effectiveness of the Transit Security Grant Program, it had not yet implemented a system to collect performance information or to report performance results. Additionally, we reported that the two agencies that manage the Transit Security Grant Program—TSA and FEMA—lacked defined roles and responsibilities, as there was no memorandum of understanding or similar document articulating the roles and responsibilities of the agencies. In June 2011, the DHS IG also reported that TSA did not require Amtrak to develop a corrective action plan addressing the highest ranked vulnerabilities, and TSA approved Amtrak investment justifications for lower risk vulnerabilities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00799 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.425

		Among other things, we and the DHS IG made various recommendations, including that DHS strengthen its methodology for determining risk; incorporate systems to collect information necessary to measure the effectiveness of the Transit Security Grant Program; define TSA's and FEMA's respective roles and responsibilities for managing the Transit Security Grant Program in a memorandum of understanding or similar document; and work closely with Amtrak to establish a corrective action plan and internal procedures that ensure decisions to fund Amtrak rail station remediation projects focus on mitigating the highest vulnerabilities identified by risk assessments. DHS concurred and took steps to address them. For example, TSA and FEMA signed a memorandum of understanding defining roles and responsibilities in March 2011. TSA also reported in July 2011 that the performance measures it developed have been incorporated into FEMA's electronic grant monitoring database and that collection of this data began with the fiscal year 2010 monitoring visits. TSA also reported updating its risk model for the grant program for fiscal year 2012 to better address vulnerability. Additionally, TSA is engaged with Amtrak to develop a comprehensive security plan. As these efforts are underway, it is too early to assess their effectiveness. We have ongoing work assessing DHS's homeland security grant programs, including the Transit Security Grant Program, and plan to report on the results of this work later this year.[f]
Information sharing	DHS expanded its efforts to share surface transportation security information by establishing information networks. However, TSA should better streamline information within and across these networks to avoid duplication as well as improve awareness of key mechanisms, and measure program effectiveness.	**DHS took steps to share surface transportation security information with stakeholders in different sectors, but should do more to streamline information-sharing mechanisms to reduce overlap, improve awareness of certain key mechanisms, and measure program effectiveness.** **Key progress:** DHS established the Homeland Security Information Network, a secure Web site that serves as a clearinghouse of information on available security technologies that have been tested and evaluated by DHS, in addition to providing security alerts, advisories, and information bulletins. Within the Homeland Security Information Network, each of the 18 critical infrastructure sectors maintains its own site, and under the transportation sector, there are sites for different transportation modes. We reported in September 2010, that 75 percent of the public transit agencies we surveyed reported being generally satisfied with the security-related information they received. Preliminary observations from interviews and open-ended responses to a survey as part of our ongoing work indicate general satisfaction among aviation, rail, and highway stakeholders.[g]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00800 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.426

	What remains to be done: We have identified challenges to DHS's surface transportation security information sharing efforts. For example, we reported in September 2010 that some public transit agencies cited the need for more streamlined information, and we identified the potential for overlap between three federal information-sharing mechanisms: the Public Transportation Information Sharing and Analysis Center,[h] the Public Transit Portal on the Homeland Security Information Network, and TSA's Office of Intelligence's page on the Homeland Security Information Network,[i] which all receive federal funding and communicate similar unclassified and security-related information to public transit agencies. We also reported that less than half of public transit agencies responding to our survey reported that they had log-in access to the Homeland Security Information Network and had not lost or forgotten their log-in information. Our survey also identified that 12 of the 19 transit agencies that did not have access to the network had never heard of it. An additional 11 agencies did not know whether they had access. Preliminary observations from interviews and open-ended responses to a survey as part of our ongoing work indicate a similar lack of access or awareness among aviation, rail, and highway stakeholders. Preliminary observations also indicate that some freight rail stakeholders would prefer to receive more analysis or actionable information from TSA that could help predict how certain events may affect rail systems. In addition, DHS and TSA have not developed performance goals and outcome-oriented measures to gauge the results of activities for the mechanisms established as primary information sources for the public transportation industry. We recommended that DHS establish time frames for a working group of federal and industry officials to assess opportunities to streamline information-sharing mechanisms to reduce any unneeded overlap and conduct targeted outreach efforts to increase awareness of the Homeland Security Information Network among agencies that are not currently using or aware of this system. We also recommended that DHS develop goals and related outcome-oriented performance measures specific to each of the three security information networks. DHS concurred, and took steps to help address the recommendations. For example, TSA and key industry groups developed a report and associated library, which is intended to streamline the analysis, sharing, and exchange of intelligence and security information that had been disseminated by multiple sources.[j] However, as we reported in June 2011, the report may reduce the number of security-related emails that public transit agencies receive, but it does not reduce overlap among the three information-sharing mechanisms. TSA officials stated that they are continuing to coordinate with other members of the working group to identify actions and time frames for addressing our recommendation, including user satisfaction and performance measures. In addition, we are continuing to assess TSA's efforts related to sharing security information with stakeholders in the aviation, rail, and highway modes and will report the final results later this year.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Visible Intermodal Prevention and Response teams employ a variety of tactics to deter terrorism, including random high-visibility patrols at mass transit and passenger rail stations using, among other things, behavior-detection officers, canine detection teams, and explosive-detection technologies.

[b] We did not independently verify the accuracy of these data.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00801 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.427

[c] The Implementing Recommendations of the 9/11 Commission Act of 2007 requires TSA to issue regulations for a training program to prepare mass transit, rail, and over-the-road bus employees for potential security threats and conditions. 6 U.S.C. §§ 1137, 1167, 1184.

[d] TSA also reported that it has distributed training products to employees in surface modes, such as a self-study training program for freight rail employees on the recognition and identification of improvised explosive devices.

[e] The Transit Security Grant Program is one of six grant programs that constitute DHS's transportation security grant portfolio. The Transit Security Grant Program provides funds to owners and operators of mass transit and passenger rail systems (which include intracity bus, commuter bus, and all forms of passenger rail, including Amtrak) to protect critical surface transportation infrastructure.

[f] We are completing this work at the request of the House Committee on Homeland Security; the Senate Committee on Homeland Security and Governmental Affairs; and the Senate Committee on Commerce, Science, and Transportation.

[g] This work is being conducted in response to a mandate in the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-35 (2007). We plan to issue our findings on this work later this year.

[h] The Public Transportation Information Sharing and Analysis Center, which is implemented by the American Public Transportation Association and funded by TSA, collects, analyzes, and distributes security and threat information from the federal government and open sources on a 24/7 basis.

[i] TSA's Office of Intelligence implemented its page on the Homeland Security Information Network in March 2010 as a collaborative information-sharing platform for all transportation modes, including public transit.

[j] The Transit and Rail Intelligence Awareness Daily report includes a daily publication to enhance situational awareness, an alert message to provide immediate awareness of a developing threat or incident, and a catalogue of supporting reports and related documents.

GAO Contact

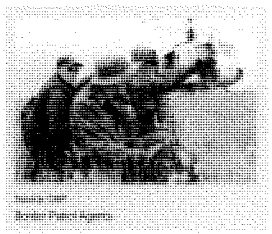
For additional information about this area, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00802 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.428

Appendix VII: Border Security

What This Area Includes



Within the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is the lead agency responsible for implementing the department's border security mission. Key areas include

- inspecting travelers at ports of entry;[1]
- inspecting cargo and goods at ports of entry while facilitating commerce;
- securing the border between ports of entry, for example, to reduce illegal immigration through the use of fencing and technology;
- enhancing visa adjudication security and preventing travel document fraud; and[2]
- collaborating with other stakeholders on border security efforts.

As the primary component responsible for border security, for fiscal year 2011, CBP had approximately 61,000 personnel and its budget authority was about $11.3 billion. Border security primarily falls within the Quadrennial Homeland Security Review Mission 2: Securing and Managing our Borders.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to border security also include managing border security resources, such as facilities, assets and human capital, we are not reporting on DHS's progress and work remaining in these areas. DHS also has other border security efforts underway on which we are not reporting. For example, CBP developed and implemented a number of border security programs and efforts to, among other things, address threats posed by the illicit narcotics trade, and acquire or develop new technologies for the southern and northern borders—such as detection sensors to detect illicit tunnels at the southern border. CBP also developed new border security strategies with Canada and Mexico. Other specific programs implemented by CBP include the Immigration Advisory

[1] Ports of entry are government-designated locations where CBP inspects persons and goods to determine, for example, whether they may lawfully enter the country. A land port of entry may have more than one border crossing point where CBP inspects travelers for admissibility into the United States.

[2] Within DHS, U.S. Immigration and Customs Enforcement (ICE) is the lead agency responsible for efforts related to enhancing visa adjudication security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00803 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.429

Program, in which CBP officers are posted at foreign airports and work with host countries' border security agencies and airlines to identify potentially inadmissible aliens, including those who may have ties to terrorism, prior to boarding commercial aircraft to the United States; and the National Targeting Center and the Automated Targeting System for identifying high-risk travelers and cargo.[3] We have not completed recent work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS has expanded its efforts in key border security areas, such as inspection of travelers, cargo, and goods at ports of entry; security of the border between ports of entry; visa adjudication and travel document security; and collaboration with other border security stakeholders. For example, our work has shown that DHS has undertaken efforts to keep terrorists and other dangerous people from entering the country, and from October 1, 2010, through June 30, 2011, CBP reported encountering over 164,000 individuals at ports of entry who were found to be inadmissible into the United States. In addition, checkpoints generally located 25 to 100 miles from the border have contributed to DHS's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. According to Border Patrol data, checkpoint operations accounted for over one-third of the Border Patrol's total drug seizures. However, our work and that of the IG have shown that key challenges remain in these efforts. For example, addressing weaknesses in port of entry traveler inspection procedures and infrastructure would increase assurance that dangerous people and illegal goods would be interdicted at the border. DHS has also not yet decided how to implement a biometric system for recording foreign nationals' exit from the United States. Further, DHS experienced schedule delays and performance problems with its information technology program for securing the border between ports of entry—the Secure Border Initiative Network (SBI*net*)—which DHS canceled. Because of the program's decreased scope, uncertain timing, unclear costs, and limited life cycle management, it was unclear whether DHS's pursuit of the program was cost-effective. DHS is

[3] The National Targeting Center vets passenger and crew manifests against information available to it to identify, for example, high-risk travelers, and identifies high-risk shipments for inspection. The Automated Targeting System is a computerized model used for targeting cargo for inspection.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00804 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.430

transitioning to a new approach for border technology, which we are assessing. DHS also should establish performance measures or management controls for key border security programs. Table 11 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 11: Assessment of Progress and Work Remaining in Key Border Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Inspection of travelers at ports of entry	CBP facilitated cross-border movement of millions of travelers while also working to keep terrorists and dangerous people from entering the country through use of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), its officer training programs, and other programs. However, weaknesses exist in traveler inspection procedures and infrastructure, and DHS does not yet have an integrated approach for tracking foreign nationals' exit from the United States.	**CBP took actions to keep terrorists and dangerous foreign nationals from entering the country at ports of entry while also facilitating the cross-border movement of millions of travelers through the use of the US-VISIT program and its officer training programs, but addressing weaknesses in these and other programs would increase assurance that dangerous people and illegal goods would be interdicted at the border.** **Key progress:** From October 1, 2010 through July 30, 2011, CBP reported encountering about 164,000 individuals at ports of entry who were found to be inadmissible into the United States, and transferred custody of more than 6,100 people with active warrants for other law enforcement purposes.[a] DHS has also undertaken an effort—the US-VISIT program— in order to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information. The entry capability has operated since 2006 at about 300 air, sea, and land ports of entry and, in November 2009, we reported that DHS had established integrated project management plans for, and had begun to interact with and involve stakeholders in, developing an exit capability. DHS reports that, through fiscal year 2011, it has been appropriated about $3.2 billion for US-VISIT.[b] As of July 2011, program officials reported that about $193 million of the appropriation had been obligated to develop air/sea and land exit solutions since 2002.[c] Further, we have work underway examining CBP's training program for CBP officers who conduct inspections at ports of entry.[d] Our preliminary observations indicate that CBP followed federal training guidelines as well as training development best practices in revising its training program for newly hired officers. In doing so, CBP addressed a previous recommendation we made that it strengthen the on-the-job portion of its training program for these newly hired officers. **What remains to be done:** We have identified weaknesses in traveler inspections and challenges to fully implementing the US-VISIT program. As we reported, from 2007 through 2011, addressing weaknesses in port of entry traveler inspection procedures and infrastructure, as well as insufficient training for CBP officers, would increase assurance that dangerous foreign nationals and illegal goods could not unlawfully enter the country; and that currency and firearms could not be smuggled out of the country and finance drug trafficking organizations and sponsors of terrorism. Although CBP's goal is to interdict all violators, CBP estimated that several thousand inadmissible aliens and other violators entered the country through ports of entry in fiscal year 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00805 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.431

Moreover, in November 2009, we reported that DHS had not adopted an integrated approach to scheduling, executing, and tracking the work that needed to be accomplished to deliver a comprehensive exit solution as part of the US-VISIT program. We concluded that, without a master schedule that was integrated and derived in accordance with relevant guidance, DHS could not reliably commit to when and how it would deliver a comprehensive exit solution or adequately monitor and manage its progress toward this end. In particular, we reported that the program faced strategic, operational, and technological challenges at land ports of entry.[8] Further, in August 2010 we reported that an exit capability was not yet implemented and that limitations in the scope, approach, and reporting of air exit pilot scenarios for the program restricted the pilots' ability to inform a decision for a long-term air exit solution.

To better provide for the successful delivery of a comprehensive US-VISIT exit solution, we recommended that DHS ensure that an integrated master schedule be developed and maintained in accordance with key practices. DHS concurred and reported, as of July 2011, that the documentation of schedule practices and procedures is ongoing, and that an updated schedule standard, management plan, and management process that are compliant with schedule guidelines are under review. DHS officials also reported that although the department operated several pilot biometric exit programs over the years and learned much from evaluations of those efforts, many challenges remain. As such, DHS stated that it continues to examine all options in connection with a final biometric air exit solution, and has recently given consideration to using its authority to establish an advisory committee to study and provide recommendations to DHS and Congress on implementing an air exit program.

In addition, preliminary observations from our ongoing work on CBP training has identified management weaknesses in its training program for incumbent officers that may be limiting CBP's ability to identify and provide the necessary training for these officers. We plan on reporting the final results of this work later this year.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00806 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.432

Inspection of cargo and goods at ports of entry while facilitating commerce	CBP improved the security and efficiency of the inspection of cargo and goods while facilitating commerce through the deployment of imaging technology and programs such as the Free and Secure Trade program. However, CBP needs to complete its study on data system enhancements.	**Through the deployment of imaging technology and programs such as the Free and Secure Trade program, CBP improved the efficiency of inspection and security of cargo and goods at ports of entry while facilitating commerce, but needs to complete a study on program benefits.** **Key progress:** CBP reported that the deployment of imaging technology at ports of entry to detect individuals hidden within vehicles, contraband, or other smuggled merchandise in vehicles and cargo had resulted in over 1,000 seizures, which included 292,000 pounds of narcotics from October 1, 2010 through June 30, 2011. In March 2011, the DHS IG reported that while CBP has policies and procedures in place, field personnel did not always receipt and record, transport, store, or dispose of seized drugs according to established policies and procedures, and in some cases, circumvented established guidance by using invalid waivers. The DHS IG attributed these conditions to insufficient oversight, communication, and staffing throughout key stages of the seizure process. Among other things, the DHS IG recommended that CBP strengthen communication and oversight to ensure field personnel comply with seizure procedures. In July 2011, DHS reported that it had implemented the recommendation to monitor personnel compliance with policies and procedures for processing drug seizures. Further, DHS officials reported using additional cargo screening measures. For example, CBP reported that it used large-scale X-ray and gamma ray imaging systems to perform examinations of cargo without having to unload cargo for manual searches or examination of conveyances by methods such as drilling or dismantling. In addition, DHS reported that it began screening 100 percent of southbound rail shipments for unlawful smuggling of weapons, drugs, and cash. Further, to facilitate the travel of low-risk screened shipments across the border and expedited border processing, the United States and Canada participate in the Free and Secure Trade program.[1] In July 2010, we reported that CBP officials and stakeholders we interviewed said that wait times for commercial vehicles traveling across the border into the U.S. had generally decreased under this program. **What remains to be done:** In July 2010, we reported that CBP lacked data needed to assess whether participants in the Free and Secure Trade program experienced intended program benefits, such as expedited border processing. Among other things, we recommended that CBP conduct a study to determine if program benefits are being realized. As we reported, such a study would enable CBP to determine if the benefits are experienced by all program participants and what program adjustments, if any, are needed. DHS concurred and reported in July 2011 that once the enhancements to its data systems were complete, it would conduct a study within 120 days to determine whether the program was meeting its intended benefits. DHS estimates completion of this study in October 2011. While these plans are positive, it is too early to assess the results of DHS's effort until the study is completed.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00807 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.433

Security of the border between ports of entry	DHS deployed technologies to secure the border between ports of entry and reduce illegal immigration. In addition, checkpoints contributed to Border Patrol's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. However, DHS has experienced schedule delays and significant performance problems with the technology portion of the Secure Border Initiative and should improve its implementation of checkpoints through enhanced design, staffing, and performance measurement.	**DHS deployed technologies to secure the border between ports of entry and reduce illegal immigration, but DHS experienced schedule delays and significant challenges with meeting cost-effectiveness and viability standards for these technologies.** **Key progress:** In November 2005, DHS launched the Secure Border Initiative (SBI), a multiyear, multibillion dollar program aimed at securing U.S. borders and reducing illegal immigration. Through this initiative, DHS planned to develop a comprehensive border protection system using technology, known as SBI*net*, and tactical infrastructure—fencing, roads, and lighting. In March 2011, we reported that surveillance capability deployed through this initiative was being used in Arizona, and that the CBP Office of Border Patrol considered these capabilities to be useful, for example, by providing continuous surveillance in border areas where none existed before. In addition, in May 2010 we reported that CBP had completed deploying most of its planned tactical infrastructure, including 646 of the 652 miles of fencing. **What remains to be done:** Since the inception of SBI, we reported on significant management weaknesses and risks. With regard to tactical infrastructure, we reported in September 2009 that its impact on border security had not been measured and as a result, DHS was not positioned to assess the impact of this investment. Overall, DHS reported achieving an acceptable level of border control across less than half of the southwest border and less than 2 percent of the northern border during fiscal year 2010.[9] Among other things, we recommended that CBP conduct a cost-effective evaluation of the impact of tactical infrastructure. DHS generally concurred and reported actions underway to address this recommendation. For example, in June 2011, CBP stated that analysis initially conducted by the Homeland Security Institute in April 2010 on the impact of tactical infrastructure had been expanded to include other data and information, and that DHS expects to deliver a final report in February 2012.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00808 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.434

With regard to SBI*net*, in September 2008 we reported that CBP's plans to initially deploy SBI*net* technology along the southwest border had slipped from the end of 2008 to 2011. In January 2010 we reported that DHS had not effectively managed key aspects of SBI*net* testing and that DHS test plans, cases, and procedures for the test events were not defined in accordance with important elements of relevant guidance. In May 2010, we reported that because of SBI*net*'s decreased scope, uncertain timing, unclear costs relative to benefits, and limited life cycle management discipline and rigor, it was unclear whether the department's pursuit of SBI*net* was a cost effective course of action. Moreover, in October 2010 we reported that DHS needed to strengthen management and oversight of its *SBInet* contractor. Among other things we recommended (1) limiting near-term investment in the first incremental block of SBI*net*,[h] (2) economically justifying any longer-term investment in SBI*net*, and (3) improving key program management disciplines. DHS generally agreed with our recommendations. In January 2011, the Secretary of Homeland Security directed CBP to end the SBI*net* program as originally conceived because it did not meet cost-effectiveness and viability standards, and to instead focus on developing solutions utilizing existing, proven technology, such as camera-based surveillance systems, for each border region. Given that DHS is transitioning to a new approach—the Alternative (Southwest) Border Technology plan—we and DHS are assessing the extent to which the issues we identified with respect to SBI*net* are applicable to the new plan.

The Alternative (Southwest) Border Technology plan is to incorporate a mix of technology, including an Integrated Fixed Tower surveillance system similar to that used in the current SBI*net* capability, beginning with high-risk areas in Arizona. In March 2011, we reported that due to a number of reasons, the cost-effectiveness and operational effectiveness and suitability of the Integrated Fixed Tower system was not yet clear. First, the analysis of alternatives DHS used to inform its decision to cancel SBI*net* cited a range of uncertainties, and it was not clear how the analyses and conclusions were factored into planning and budget decisions regarding the optimal mix of technology deployments in Arizona. Second, independent analyses conducted by the Army's Test and Evaluation Command were not complete at the time of the Secretary's decision to cancel SBI*net*, thus any results on SBI*net*'s operational effectiveness and suitability could not inform the decisions to proceed with the Integrated Fixed Tower system. DHS did not agree with our observations on the analysis of alternatives and the potential usefulness of the Army's Test and Evaluation Command. We believe our observations are valid.

Checkpoints contributed to the Border Patrol's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. However, the need to strengthen checkpoint design and staffing, and improve the measurement and reporting of checkpoint effectiveness has impeded higher levels of performance.

Key progress: CBP's Border Patrol uses checkpoints to protect the nation from the impact of contraband illegally smuggled across the border, and from removable aliens, some of whom may have ties to organized crime or countries at a higher risk of having groups that sponsor terrorism. In August 2009 we reported that checkpoints had contributed to the Border Patrol's ability to seize illegal drugs, apprehend removable aliens, and encounter known or suspected terrorists. Moreover, checkpoint operations accounted for over one-third of the Border Patrol's total drug seizures, according to Border Patrol data.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00809 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.435

		What remains to be done: In August 2009, we reported on factors that impeded higher levels of performance with regard to checkpoints. For example, Border Patrol officials we spoke with said that additional staff, canine teams, and inspection technology were needed to increase checkpoint effectiveness. In addition, we reported that a lack of management oversight and unclear checkpoint data collection guidance resulted in the overstatement of checkpoint performance results in fiscal year 2007 and 2008 agency performance reports, as well as inconsistent data collection practices at checkpoints. Moreover, Border Patrol was not yet using performance measures it had developed to examine the extent to which checkpoint operations affected quality of life in surrounding communities. We recommended that CBP strengthen checkpoint design and staffing, and improve the measurement and reporting of checkpoint effectiveness, including community impact. Implementing performance measures would serve to provide greater attention and priority in Border Patrol operational and staffing decisions to address any existing issues at checkpoints and strengthen program accountability. CBP concurred and has reported actions underway to address them. For example, in July 2011 CBP reported that it had acquired the services of the DHS Science and Technology Centers of Excellence (University of Arizona and University of Texas, El Paso) to assist in measuring the effectiveness of checkpoints, and to assess the economic and social impacts of permanent checkpoints on the surrounding communities. DHS officials expect a final report on or about the end of fiscal year 2012.
Visa adjudication security and preventing travel document fraud	DHS improved programs designed to enhance visa security, including the Visa Security Program, Visa Waiver Program, and the Western Hemisphere Travel Initiative. However, further steps are needed to evaluate these efforts, address potential risks, and enhance training and oversight.	**DHS contributed to the enhancement of visa adjudication security; however, further steps are needed to evaluate these efforts.** **Key progress:** In March 2011, we reported that the DHS Visa Security Program, which is administered by U.S. Immigration and Customs Enforcement (ICE), is a part of the visa screening process at certain embassies and consulates in which ICE personnel review visa applications to help prevent individuals who pose a threat from entering the United States. The Visa Security Program is currently deployed to 19 posts in 15 countries. Moreover, we reported that ICE had developed a 5-year expansion plan in 2007 for the Visa Security Program. In addition, in August 2011, CBP reported that it had implemented a new program for continuously vetting recently issued U.S. nonimmigrant visas for derogatory information that becomes available subsequent to visa issuance. CBP reported that if it uncovers such derogatory information, it alerts the Department of State that the traveler may no longer be eligible for the visa.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00810 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.436

What remains to be done: In March 2011, we reported that ICE needed to improve performance evaluation of the Visa Security Program and better address visa risk worldwide. Specifically, we reported that ICE could not accurately assess progress toward its program objectives because, among other things, the tracking system it used to collect data on program activities did not gather comprehensive data on all the performance measures needed to evaluate mission objectives. Moreover, we reported that ICE did not fully follow or update its 5-year expansion plan. For instance, ICE did not establish 9 posts identified for expansion in 2009 and 2010, and had not taken steps to address visa risk at posts that did not have a Visa Security Program presence. We made recommendations designed to address these weaknesses. DHS concurred with some of these recommendations, and stated that it is taking steps to address them. For example, DHS stated that it is identifying alternatives for Visa Security Program review at high risk posts that do not have a physical Visa Security Program presence. DHS did not concur with other recommendations, including that the program collect comprehensive data on all performance measures and track the time spent on visa security activities. DHS stated that the Visa Security Program captured all of the required performance metrics identified in its 5-year expansion plan. However, we reported that while ICE was collecting some data on the performance measures identified in its plan, our analysis showed that the data were not sufficient to accurately demonstrate the progress made toward achieving program objectives.

DHS has taken steps intended to enhance the security of the Visa Waiver Program, which enables eligible citizens of participating countries to travel to the United States without first obtaining a visa, but has not yet fully evaluated and addressed program risks.

Key progress: In May 2011, we reported that DHS had implemented an electronic authorization system for screening and determining the eligibility of potential visa waiver travelers in advance of their travel—the Electronic System for Travel Authorization. In May 2011, we reported that DHS requires that Visa Waiver Program countries enter into information-sharing agreements with the United States; however, only half of the countries fully complied with this requirement and many of the signed agreements had not been implemented. Half of the countries had entered into agreements to share watchlist information about known or suspected terrorists and to provide access to biographical, biometric, and criminal history data. Almost all of the 36 Visa Waver Program countries had entered into an agreement to report lost and stolen passports. DHS, with the support of interagency partners, had established a compliance schedule requiring the last of the Visa Waver Program countries to finalize these agreements by June 2012.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00811 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.437

What remains to be done: In May 2011, we reported that DHS had not fully evaluated security risks related to the small percentage of Visa Waiver Program travelers without verified approval by the system to know to what extent they posed a risk to the program.[i] Moreover, we reported that DHS had not completed 18 of the 36 most recent required reports on Visa Waiver Program countries' security risks in a timely manner, and as result, it was unclear whether vulnerabilities existed that jeopardized continued participation in the Visa Waiver Program.[j] We recommended that DHS establish time frames for the regular review of cases of Electronic System for Travel Authorization noncompliance and address delays in the biennial country review process to ensure timely completion. DHS concurred with our recommendations, and in July 2011 DHS stated that it established procedures to perform quarterly reviews of a representative sample of Visa Waiver Program passengers who do not comply with the Electronic System for Travel Authorization requirement to determine the level of risk posed to Visa Waiver Program security and identify improvements to minimize noncompliance. While these are positive steps, as DHS has just taken these actions, it is too early to assess their impact.

DHS improved the Western Hemisphere Travel Initiative, but this initiative would be strengthened by enhanced training, oversight, and guidance.

Key progress: The Western Hemisphere Travel Initiative required, as of June 1, 2009, for land and sea travel and as of January 23, 2007, for air travel, certain travelers who previously were allowed to enter the United States from within the Western Hemisphere without passports to present passports or other approved documents to enter the United States.[k] According to DHS, the Western Hemisphere Travel Initiative improved CBP's ability to identify individuals misrepresenting themselves or falsely claiming U.S. citizenship. In February 2011, the DHS IG reported that CBP successfully implemented these requirements in the air environment, and because the requirements improved CBP officers' ability to validate the identity and citizenship of compliant air passengers, officers were able to spend more time inspecting travelers without passports. In addition, CBP reported the average inspection process time as having been reduced since implementation of the Western Hemisphere Travel Initiative and that this initiative has promoted more efficient processing of travelers into the United States.

What remains to be done: The DHS IG reported that, due to inadequate incumbent officer training, oversight, and guidance, there was insufficient assurance that CBP officers verified the identity and citizenship of all individuals who did not provide a passport or other compliant documentation. In addition, the DHS IG recommended, among other things, that CBP implement procedures for monitoring CBP officers' compliance with Western Hemisphere Travel Initiative enforcement procedures. DHS concurred and identified actions to implement procedures for monitoring compliance. For example, in July 2011 CBP reported that it plans to clarify and reissue guidance and provide refresher training to CBP officers on Western Hemisphere Travel Initiative compliance and procedures for noncompliant travelers by September 2011. In addition, CBP reported that it planned to implement procedures for monitoring CBP officers' compliance with CBP policy regarding the Western Hemisphere Travel Initiative enforcement procedure using CBP's Self Inspection Program by December 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00812 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.438

Collaborating on border security efforts	DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts through interagency forums and joint operations. However, DHS should strengthen cooperation through enhanced oversight to ensure efficient use of interagency forums and improved information sharing.	**DHS improved collaboration with federal, state, local, tribal, and international partners on northern border security efforts such as interagency forums, but should strengthen cooperation through better oversight of these forums and information sharing.** **Key progress:** In December 2010 we reported that federal, state, local, tribal, and international law enforcement partners reported improved DHS coordination to secure the northern border. For example, interagency forums helped in establishing a common understanding of border security threats, while joint operations helped to achieve an integrated and effective law enforcement response. **What remains to be done:** We found that more work remains in sharing information and resources useful for operations for northern border security. For example, partners in all four sectors we visited cited ongoing challenges sharing information and resources for daily border security, and that oversight by management at the component and local level has not ensured consistent compliance with provisions of interagency agreements, such as those related to information sharing. Among other things, we recommended that DHS enhance oversight to ensure the efficient use of interagency forums and compliance with interagency agreements. DHS concurred and has taken steps to address the recommendations, such as reviewing the inventory of interagency forums through its strategic and operational planning efforts to assess efficiency and identify challenges. DHS officials reported in July 2011 that the department plans to release a strategy that will articulate a department-level approach to more efficiently and effectively secure and manage the U.S. northern border. Officials reported that this overarching framework will emphasize intra-DHS coordination as well as enhanced collaboration with federal, state, local, tribal, territorial and Canadian partners. The department is still determining the best path forward for implementing the goals of the strategy, and stated that any implementation effort will require enhanced coordination between DHS components, including CBP Office of Border Patrol and ICE, as well as improved cooperation with partners on both sides of the border.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] CBP's Office of Field Operations reported that of the total individuals at ports of entry who were found to be inadmissible into the United States, 55,903 were at the southern land border and 24,066 were at the northern land border. The remaining inadmissible individuals were at sea ports (52,366), air ports (29,049), and other uncategorized inadmissible events (2,818). We did not independently verify the accuracy of these data.

[b] DHS was appropriated about $335 million for US-VISIT for fiscal year 2011. Pub. L. No. 112-10, § 1829, 125 Stat. 38, 143 (2011).

[c] We did not independently verify the accuracy of these data.

[d] We are conducting this work for the House Committee on Homeland Security.

[e] GAO, *Border Security: US-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry*, GAO-07-248, Washington, D.C.: Dec. 6, 2006.

[f] The United States and Mexico also participate in the Free and Secure Trade program, but the focus of our report was on United States and Canada participation. CBP launched the Free and Secure Trade program in 2002 to expedite processing for pre-vetted, low-risk shipments. The program is intended to secure and facilitate legitimate trade by providing expedited processing of participants' merchandise in designated traffic lanes at select border sites, result in fewer referrals to secondary inspections, enable "front-of-the-line" processing in secondary CBP inspections, and provide for enhanced security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00813 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.439

[g] According to Border Patrol, an acceptable level of border control is established when it has the capability (i.e., resources) to deter or detect and apprehend incursions at the immediate border or after entry.

[h] SBI*net* was being acquired and deployed in incremental blocks of capability, with the first block to cost about $1.3 billion.

[i] Specifically, we reported that in 2010, airlines complied with the requirement to verify Electronic System for Travel Authorization approval for almost 98 percent of Visa Waiver Program passengers prior to boarding, but the remaining 2 percent—about 364,000 travelers—traveled under the Visa Waiver Program without verified Electronic System for Travel Authorization approval.

[j] The Enhanced Border Security and Visa Entry Reform Act of 2002 increased the frequency—from once every 5 years to at least once every 2 years—of mandated assessments of the effect of each country's continued participation in the Visa Waiver Program on the security, law enforcement, and immigration interests of the United States. The law also directs DHS to determine, based on the evaluation, whether each Visa Waiver Program country's designation should continue or be terminated and to submit a written report on that determination to select congressional committees. 8 U.S.C. § 1187(c)(5)(A)(i).

[k] In July 2008, the Department of State began issuing passport cards as a lower-cost alternative to passports for U.S. citizens to meet Western Hemisphere Travel Initiative requirements. In October 2008, the Department of State began issuing the second generation border crossing card based on the architecture of the passport card. In June 2010 we reported that improvements in the Department of State's development process could increase the security of these documents. See GAO, *Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards*, GAO-10-589, Washington, D.C.: June 1, 2010.

GAO Contact

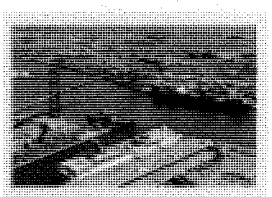
For additional information about this area, contact Richard M. Stana at (202) 512-8816 or stanar@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00814 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.440

Appendix VIII: Maritime Security

What This Area Includes



Source: U.S. Coast Guard
Port of Los Angeles

Within the Department of Homeland Security (DHS), the U.S. Coast Guard has primary responsibility for maritime security, while various component agencies also contribute to maritime security efforts, including U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and the Domestic Nuclear Detection Office (DNDO).[1] Key areas within maritime security include (1) port facility and vessel security; (2) maritime domain awareness and information sharing; and (3) international supply chain security. The Coast Guard is responsible for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain. In this capacity, among other things, it conducts port facility inspections, leads the coordination of maritime information sharing efforts, and promotes domain awareness in the maritime environment. CBP is responsible for the maritime screening of incoming commercial cargo for the presence of contraband, such as explosives, while facilitating the flow of legitimate trade, cargo, and passengers. TSA and the Coast Guard have responsibility for the implementation and enforcement, respectively, of the Transportation Worker Identification Credential program to manage the access of maritime workers to regulated maritime facilities. DNDO is responsible for acquiring and supporting the deployment of radiation detection equipment, including portal monitors. As one of the primary components responsible for maritime security protection, for fiscal year 2011 the Coast Guard had about 50,000 personnel, including civilian and military, and its budget authority was about $10.2 billion.[2] Maritime

[1] U.S. Immigration and Customs Enforcement (ICE) also contributes to maritime security in that its mission is to detect and prevent terrorist and criminal acts by targeting the people, money, and materials that support terrorist and criminal networks. In this capacity, ICE contributes to DHS border security efforts, including in the maritime environment, even though its main focus is not interdicting or screening operations.

[2] The budget and personnel figures for Coast Guard include its nonhomeland security related programs, such as its search and rescue mission function. In addition to Coast Guard resources, for fiscal year 2011 CBP had about 61,000 personnel and budget authority of about $11.4 billion; TSA had about 55,000 personnel and budget authority of about $7.7 billion; and the DNDO had about 130 personnel and budget authority of about $340 million. However, the figures for these components include their nonmaritime security related programs for fiscal year 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00815 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.441

security primarily falls within the Quadrennial Homeland Security Review Mission 2: Securing and Managing our Borders.[3]

For the purposes of this report, we are generally focusing on key areas on which we and the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to maritime security also include maritime security national planning, we are not discussing DHS's progress and work remaining in this area. DHS has developed and implemented other efforts related to maritime security. For example, according to the Coast Guard, its maritime security programs are part of a layered strategy that begins far from our ports. Coast Guard officials noted that their security regime includes close coordination with international and regional organizations (such as the International Maritime Organization and the European Union), and individual country's coast guard equivalent agencies; security inspections of, and technical assistance to, foreign ports; and maintaining a multi-mission fleet of cutters patrolling our coastal approaches. The Coast Guard also noted that some of its other missions—those not directly part of its ports, waterways, and coastal security mission—can contribute to homeland security.

Further, in July 2011, the Coast Guard reported that it had specific initiatives underway to enhance maritime security planning at the port level, on which we have not previously reported. Specifically, Coast Guard reported that it had updated 43 port-level Area Maritime Security Plans that covered prevention, protection, security response, and short-term recovery, and that these plans were approved by Coast Guard district and area commanders. The Coast Guard further reported that it was working closely with maritime committees and stakeholders to maintain and annually exercise these port-level plans. We have not completed work on these areas upon which to make an assessment.

[3] While Coast Guard's maritime security efforts reported by us and the DHS IG primarily fall within Mission 2 of the Quadrennial Homeland Security Review, according to Coast Guard, its port level maritime security planning efforts fall within Mission 1: Preventing Terrorism and Enhancing Security and Mission 5: Ensuring Resilience to Disasters. For the purposes of this report, we discussed Coast Guard's port level security planning efforts under the maritime security functional area aligned under QHSR Mission 2, as discussed in appendix II on our scope and methodology.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00816 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.442

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS's components, particularly the Coast Guard and CBP, have expanded their efforts in key areas, such as port facility and vessel security; maritime domain awareness and information sharing; and international supply chain security. The Coast Guard strengthened risk management through the development of a risk assessment model, and developed a strategy and programs intended to address risks to maritime facilities and passenger and commodity vessels. In addition, the Coast Guard increased maritime domain awareness through interagency operational centers, implementing a vessel tracking system, and identifying awareness gaps in the Arctic.[4] For example, in July 2011, DHS reported that it had completed an interagency review of maritime domain awareness requirements resulting in the publication of a document that included key strategic capabilities, objectives, resources, and evaluative methods needed to maintain maritime domain awareness. Further, in July 2011 DHS reported that CBP developed the Small Vessel Reporting System to allow for better tracking of small boats arriving from foreign locations, and deployed this system to eight of CBP's field locations. DHS also developed a layered security strategy for cargo container security, including deploying screening technologies and partnering with foreign governments.

However, our work and that of the DHS IG has shown that more work remains. For example, DHS components' efforts to assess the effectiveness of programs to secure maritime facilities should be improved. We found that because of a lack of technology capability, DHS does not electronically verify identity and immigration status of foreign seafarers as part of its admissibility inspection process, thus limiting the assurance that fraud could be identified among documents presented by them. DHS also had not assessed the risks of not having this capability, which is not expected to be available for several years. Further, DHS and its partners should enhance efforts to improve maritime domain awareness by, for example, further strengthening tracking of small vessels. In addition, although DHS developed the Transportation Worker Identification Credential program, we found that the program's controls were not designed to provide reasonable assurance that only qualified applicants acquire credentials. For example, during covert tests of the

[4] Interagency operational centers are one element of maritime domain awareness, for which other agencies, particularly the Department of Defense, also have responsibilities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00817 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.443

Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Table 12 provides more detailed information on our assessment of DHS's progress and work remaining in key areas on which we have reported, with an emphasis on work completed since 2008.

Table 12: Assessment of Progress and Work Remaining in Key Maritime Security Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Port facility and vessel security	The Coast Guard strengthened security of port facilities and vessels by developing a risk assessment model; conducting annual inspections; working to prevent unauthorized entry of individuals; and providing additional efforts to secure passenger and commodity vessels. However, the information system for tracking inspections and efforts to assess the effectiveness of security measures should be improved.	**The Coast Guard strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. However, difficulties in calculating effects may challenge its ability to conduct risk assessments.** **Key progress:** The Coast Guard strengthened risk management through the development of a risk assessment model to help prioritize limited port security resources. In July 2010 we noted that the Coast Guard made progress assessing risks by developing the Maritime Security Risk Analysis Model, which is used to assess risk to individual assets and facilities within ports. It is used by each Coast Guard sector, and assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios. The Coast Guard is starting to integrate the results of its risk assessment efforts into resource allocation decisions, including informing decisions about deployment of local assets. Additionally, the Coast Guard is starting to use the Maritime Security Risk Analysis Model results for evaluating capabilities needed to combat future terrorist threats and identifying the highest-risk scenarios and targets in the maritime domain. For example, Coast Guard officials reported that the results of the risk assessments were used to refine the Maritime Security and Response Operations requirements for the number of cruise ship escorts and patrols of cruise ship facilities.[a] In July 2011, the Coast Guard reported that it had worked with DNDO to add radiological and nuclear threats to the Maritime Security Risk Analysis Model scenarios. **What remains to be done:** We are conducting work examining the Maritime Security Risk Analysis Model, as well as reviewing the role that risk plays in the allocation of resources in the Port Security Grant Program.[b] In August 2011, we testified on the use of the Maritime Security Risk Analysis Model to assess offshore energy facilities. We found that the Coast Guard has several limitations in assessing the risks to such facilities. Such limitations involve calculating secondary economic effects and assessing the systematic or network risks of an attack on offshore energy facilities. We plan to report the results from our ongoing work later this year.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00818 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.444

Area	Overall assessment	Summary of key progress and work remaining
		DHS addressed risk to port facilities through annual inspections and efforts to prevent unauthorized entry of individuals. However, risks exist in not electronically verifying the identity and immigration status of foreign seafarers onboard cargo vessels. **Key progress:** DHS has addressed risks to port facilities through annual inspections and programs designed to prevent the unauthorized entry of individuals. Federal law requires certain port facilities to have security plans in place.[c] Coast Guard guidance calls for at least one announced annual inspection and at least one unannounced annual spot check to ensure that plans are being followed. In February 2008, we reported that Coast Guard's inspections were identifying and correcting facility deficiencies. For example, the Coast Guard identified deficiencies in about one-third of the facilities inspected from 2004 through 2006, with deficiencies concentrated in certain deficiency categories, such as failing to follow facility security plans for access control. We are currently conducting work examining, among other things, the way in which the Coast Guard assesses risk and ensures security of offshore energy infrastructure.[d] As part of our review, we plan to analyze offshore infrastructure security plans and the Coast Guard's security inspection reports. We plan to report the final results from this effort later this year. In August 2011, we testified that the Coast Guard should strengthen its internal controls to ensure that required risk assessments are done at appropriate offshore infrastructure. Further, DHS took actions to address risks posed by unauthorized individuals with access to U.S. port facilities. Specifically, in January 2011, we reported on actions the Coast Guard and CBP took to address risk posed by foreign seafarers entering U.S. seaports. We found that the agencies were using a layered security strategy for identifying and addressing risks, and that CBP and the Coast Guard were conducting advance-screening, inspections, and enforcement operations. For example, both CBP and the Coast Guard received and screened advance information on commercial vessels scheduled to arrive at U.S. ports, and prepared risk assessments based on the results of the advance-screening of vessel and seafarer information. We also reported that the Coast Guard may conduct armed security boarding of arriving commercial vessels based on various factors, including intelligence it received to examine seafarer passports and visas, among other things, and ensure the submitted crew list is accurate. In addition, we have reviewed DHS's efforts to manage the access of maritime workers to regulated maritime facilities through the Transportation Worker Identification Credential program. For example, in May 2011, we reported that TSA designed processes to facilitate the issuance of credentials to maritime workers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00819 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.445

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: With regard to foreign seafarers, in January 2011 we reported that because of a lack of technology capability, DHS did not electronically verify identity and immigration status on board cargo vessels, thus limiting assurance that fraud was identified among documents presented by foreign seafarers seeking admission into the United States. DHS also had not assessed the risks of not having this capability, which is not expected to be available for several years. Further, we reported that DHS faced challenges in ensuring it had reliable data on illegal entries by foreign seafarers at U.S. seaports. For example, both CBP and the Coast Guard track the frequency of absconder (a seafarer CBP has ordered detained on board a vessel in port, but who departs a vessel without permission) and deserter (a seafarer CBP grants permission to leave a vessel, but who does not return when required) incidents at U.S. seaports, but the records of these incidents varied considerably among the two agencies. As a result, the data DHS used to inform its strategic and tactical plans were of undetermined reliability. We recommended that DHS assess the risks of not electronically verifying foreign seafarers for admissibility, and that CBP and the Coast Guard determine why their data varied and jointly establish a process for sharing and reconciling records of illegal seafarer entries at U.S. seaports. DHS concurred and reported that CBP met with the DHS Screening Coordination Office to determine risks associated with not electronically verifying foreign seafarers for admissibility. Further, in July 2011 DHS reported that CBP and the Coast Guard were working to assess the costs associated with deploying biometric capabilities to the maritime domain. As these efforts are in the early stages, it is too soon to assess their results. Further, given the number of seafarers transiting U.S. ports each year and the continued threats posed by terrorism to the United States, establishing a process for sharing and reconciling information on absconder and deserter incidents could better support Coast Guard's and CBP's efforts to prevent illegal immigration at U.S. seaports. With regard to the Transportation Worker Identification Credential, in May 2011 we reported that program controls were not designed to provide reasonable assurance that only qualified applicants could acquire the credentials. For example, during covert tests of the Transportation Worker Identification Credential at several selected ports, our investigators were successful in accessing ports using counterfeit credentials and authentic credentials acquired through fraudulent means. Further, DHS had not assessed the program's effectiveness at enhancing security or reducing risk for federally regulated facilities. We recommended, among other things, that DHS assess the program's internal controls to identify needed corrective actions, assess its effectiveness, and use the information to identify effective and cost-efficient methods for meeting program objectives. DHS concurred and stated that it has initiated a review of current Transportation Worker Identification Credential program internal controls with a specific focus on the controls highlighted in our May 2011 report. As DHS is in the early stages of implementing these actions, it is too early to assess their impact. Until such efforts are completed, it will be difficult for DHS to provide reasonable assurance that the program is meeting its goals and that only qualified applicants can acquire the credentials.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00820 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.446

Area	Overall assessment	Summary of key progress and work remaining
		The Coast Guard conducted pre-entry security boarding, escorts, and patrols to secure passenger and commodity vessels, but additional actions and further study are needed. **Key progress:** DHS took measures to help secure vessels including cruise ships, ferries, and energy commodity vessels such as tankers. In April and December 2010, we reported that DHS assessed risks to cruise ships and ferries, respectively, and in December 2007 we reported that DHS took action to prevent and be prepared to respond to attacks on energy commodity tankers. We also reported that DHS took measures to better secure these vessels. For example, the Coast Guard provided escorts for cruise ships to help prevent waterside attacks and a security presence on ferries during transit. CBP conducted reviews of passenger and crew data for terrorist connections or criminal ties and helped to ensure that all passengers and crew are cleared for entry into the United States. Further, with regard to energy commodity tanker security, the Coast Guard conducted security activities, such as pre-entry security boardings, escorts, and patrols. **What remains to be done:** DHS made progress in these areas, but additional actions are needed to further enhance security. For example, we reported that CBP had not assessed the costs and benefits of requiring cruise lines to provide passenger reservation data for screening, which could help improve identification and targeting of potential terrorists. Additionally, Coast Guard records showed that at some ports, a lack of resources hindered some Coast Guard units from meeting their self-imposed requirements for activities, such as escorts and boardings to secure tankers. We recommended, among other things, that CBP conduct a study to determine whether requiring cruise lines to provide automated passenger data to CBP on a systematic basis would benefit homeland security. We also recommended that DHS develop a national resource allocation plan to balance the Coast Guard's security responsibilities to protect energy commodity vessels with its other mission functions. DHS concurred with our recommendations and reported taking steps to address them. In July 2011, CBP reported that it had conducted site surveys at three ports of entry to assess the advantage of having cruise line booking data considered in a national targeting process, and had initiated discussions with a cruise line association on the feasibility of CBP gaining national access to cruise line booking data. Although CBP had originally set a due date of June 30, 2011, for its full evaluation of these issues, CBP reported that it had requested an extension to September 30, 2011, to obtain information from the cruise industry on potential impacts of requiring them to provide passenger data on a systematic basis. In addition, Coast Guard officials stated that they plan to develop a resource allocation plan, starting in April 2012, as part of the implementation of a national strategy, which is being developed for reducing the maritime security risks present in the bulk transportation and transfer of certain dangerous cargo on commodity vessels. In the interim, the Coast Guard has published guidance to clarify the process' timing and scope to ensure full consideration is given to safety and security of the port, the facility, and the energy commodity vessel. We have reported that actions such as these are important to help ensure that the Coast Guard is positioning itself to address threats to passenger and commodity vessels. As CBP and the Coast Guard are in the early stages of implementing these efforts, it is too soon to assess their effectiveness.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00821 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.447

Area	Overall assessment	Summary of key progress and work remaining
Maritime domain awareness and information sharing	DHS strengthened maritime domain awareness through efforts such as establishing interagency operations centers, vessel tracking systems, and identifying security gaps in the Arctic. However, these efforts face challenges including budgetary constraints, difficulty tracking smaller and noncommercial vessels, and the need for improved information sharing with key Arctic stakeholders.	**DHS and its partners are working to establish interagency operations centers to improve maritime domain awareness, but these efforts face budgetary constraints and other challenges.** **Key progress:** The Security and Accountability For Every Port Act of 2006 calls for the establishment of interagency operations centers for port security, directing the Secretary of DHS to establish such centers at all high-priority ports no later than 3 years after the act's enactment (enacted October 13, 2006).[8] In October 2007, we reported that Coast Guard was piloting various aspects of future interagency operations centers at its 35 existing command centers and working with multiple interagency partners to further their development. According to the Coast Guard, future interagency operations centers would allow the Coast Guard and its partners to use port surveillance with joint tactical and intelligence information and share these data with port partners working side by side in expanded facilities. In July 2011, DHS reported that it had completed an interagency review of maritime domain awareness requirements which resulted in the publication of a document that included key strategic capabilities, objectives, resources, and evaluative methods needed to maintain maritime domain awareness. **What remains to be done:** In October 2007, we reported that the Coast Guard faced budget constraints in trying to expand its current command centers and include other agencies at the centers. In our ongoing work looking at the continued implementation of Interagency Operations Centers, our preliminary observations indicate that as of August 2011, the Coast Guard has installed its information sharing system at more than 10 Coast Guard sectors.[f] Based on our preliminary observations, we identified concerns about whether the Coast Guard will meet its goals related to the involvement of port partners. We plan to report the final results of our work later this year.
		DHS implemented vessel-tracking systems, but tracking small vessels poses challenges. **Key progress:** At sea or in U.S. coastal areas, inland waterways, and ports, the Coast Guard relies on a diverse array of vessel tracking systems operated by various entities. For tracking vessels at sea, the Coast Guard uses a long-range identification and tracking system, and a commercially provided long-range automatic identification system.[9] For tracking vessels in U.S. coastal areas, inland waterways, and ports, the Coast Guard operates a land-based automatic identification system, and also either operates, or has access to, radar and cameras in some ports. In addition, in July 2011, DHS reported that CBP developed the Small Vessel Reporting System to allow for better tracking of small boats arriving from foreign locations, and deployed this system to eight of CBP's field locations. Among other things, DHS reported that this system would allow CBP to identify potential high-risk small boats to determine, for example, which needed to be boarded upon arrival.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00822 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.448

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We identified limitations in the Coast Guard's efforts to track vessels at sea. In March 2009, we reported that the means of tracking vessels at sea are potentially effective, but each has features that could impede its effectiveness. Also, the systems used in U.S. coastal areas, inland waterways, and ports—automatic identification system, radar, and video cameras—had more difficulty tracking smaller and noncommercial vessels because these vessels were not generally required to carry automatic identification system equipment, and because of the technical limitations of radar and cameras. To help address the small vessel threat, DHS developed a Small Vessel Security Strategy in April 2008, and in January 2011 issued the implementation plan for the strategy. As DHS is in the process of executing its implementation plan, it is too early to assess its effectiveness in enhancing maritime security.
		DHS identified and addressed some information gaps in the Arctic, but efforts would benefit from improved information sharing.
		Key progress: In September 2010, we reported that, according to Coast Guard officials, establishing domain awareness in the Artic would allow the Coast Guard to better understand the risks associated with operating in or monitoring the region, but that the Coast Guard faced obstacles to achieving domain awareness. Specifically, officials stated that establishing domain awareness was inhibited by (1) inadequate Arctic Ocean and weather data, (2) lack of communication infrastructure, (3) limited intelligence information, and (4) lack of a physical presence in the Arctic. The Coast Guard identified Arctic requirements and gaps for the maritime domain while also collecting relevant information from routine operations. For example, in September 2010 we reported that the Coast Guard established temporary operating locations in the Arctic and conducted biweekly Arctic overflights to obtain more information on the Arctic operating environment. In addition, information gathered during the Coast Guard's routine missions, such as ice breaking and search and rescue, informed Coast Guard requirements for operating in the Arctic region.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00823 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.449

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: The Coast Guard's success in implementing an Arctic plan rests in part on how successfully it communicates with key stakeholders, especially state and local officials, and Alaska Native tribal governments and interest groups. In September 2010 we reported that 9 of the 15 state and local officials we met with wanted more information on the status and results of the Coast Guard's efforts to develop its future Arctic requirements. For example, some state and local officials believed that the agency had already determined its plan for Arctic operations but had not shared it, and one state official reported that his office and others may be willing to invest in infrastructure that could benefit the Coast Guard if and when they know the agency's plans. Coast Guard officials told us that they have been focused on communication with congressional and federal stakeholders and intended to share Arctic plans with other stakeholders once plans are determined. In the interim, some state and local stakeholders reported having limited information that they believe would be useful on the process and progress of the agency's Arctic planning efforts. We recommended that the Coast Guard communicate with key stakeholders on the process and progress of its Arctic planning efforts. DHS concurred and in July 2011 reported it was taking actions to address our recommendation, such as soliciting comments from indigenous populations and the public on the National Ocean Policy and participating on the International Arctic Council, a high-level forum for promoting cooperation, coordination, and interaction among Arctic nations, indigenous communities, and other Arctic stakeholders on Arctic issues.[h] While these are positive steps, it is too early to assess the outcomes of DHS's consultation efforts.
International supply chain security	DHS made progress in deploying container screening technologies and partnered with foreign governments for supply chain security. However, these efforts would be enhanced by the development of measures to assess the performance of new technologies and the completion of a feasibility analysis of implementing the requirement to scan 100 percent of all U.S.-bound cargo containers.	**CBP made progress in deploying new technologies, but development and implementation of these technologies should be improved through performance standards and alignment with operational needs.** **Key progress:** DHS has made progress in developing technologies to improve container security by detecting intrusions and tracking containers and scanning them for contraband, including nuclear material. DHS conducted research and development for four container security technology projects to detect intrusion and track the movement of containers through the supply chain. For example, DHS's Science and Technology Directorate initiated the Container Security Device project to develop the capability to detect container door intrusion. Further, to detect nuclear materials, CBP, in coordination with DNDO, deployed over 1,400 radiation portal monitors at U.S. ports of entry. Most of the radiation portal monitors are installed in primary inspection lanes through which nearly all traffic and shipping containers must pass. These monitors alarm when they detect radiation coming from a package, vehicle, or shipping container. CBP then conducts further inspections at its secondary inspection locations to identify the cause of the alarm and determine whether there is a reason for concern.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00824 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.450

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We reported in September 2010 that DHS had not yet developed performance standards for these new technologies because it had not yet demonstrated that they can effectively work in operational environments. Additionally, DNDO began working on the cargo advanced automated radiography system with the intention that this technology could be used to detect a variety of contraband, including shielded nuclear materials, in vehicles and containers at U.S. ports of entry. However, we reported that the office did so without fully understanding that the technology would not fit within existing primary inspection lanes at CBP ports of entry.[1] We identified lessons learned for DHS to consider in its future acquisition efforts, such as to (1) engage in a robust departmental oversight review process, (2) separate the research and development functions from acquisition functions, (3) determine the technology readiness levels before moving forward to acquisition, and (4) rigorously test devices using actual agency operational tactics before making decisions on acquisition. DHS announced the termination of the program in September 2010. DNDO also tested next-generation radiation-detection equipment, or advanced spectroscopic portals, used to detect smuggled nuclear or radiological materials. We reported in June 2009 that while DNDO increased the rigor of testing the new monitors in comparison with previous tests and thereby added credibility to the test results, the benefits of the monitors may not justify the high cost. In July 2011, the Director of DNDO testified that because the original design specification for advanced spectroscopic monitors program does not adequately reflect the operational needs in the field, and because there are now competing commercially-available portal radiation detection systems, DHS was ending the program as originally conceived. DHS reported that it plans to deploy the existing units to field locations to gather operational data to support future planning efforts.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00825 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.451

Area	Overall assessment	Summary of key progress and work remaining
		DHS developed and implemented programs to partner with foreign governments to inspect suspicious cargo before it leaves for U.S. ports, but these programs should be improved through enhanced planning such as feasibility analyses and oversight. **Key progress:** DHS implemented programs to inspect suspicious cargo before it leaves for U.S. seaports. For example, CBP established partnerships with members of the international trade community, including the private sector through its Customs-Trade Partnership Against Terrorism, and with foreign governments through its Container Security Initiative and Secure Freight Initiative. The Container Security Initiative program places CBP staff at participating foreign ports to partner with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States, and the Secure Freight Initiative is a program at selected ports with the intent of scanning 100 percent of U.S.-bound container cargo for nuclear and radiological materials overseas. DHS reported that, as of July 2011, the Container Security Initiative was operational at 58 ports worldwide. CBP and its international partners also developed the World Customs Organization's Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework). In February 2010, the DHS IG reported on CBP's management and oversight of the Container Security Initiative program. The DHS IG noted that CBP had used proactive management and oversight processes through the Container Security Initiative to identify and inspect high-risk cargo at foreign ports. The IG further reported that CBP conducts periodic evaluations of overseas Container Security Initiative operations and has software tools to help managers monitor port activities. **What remains to be done:** We reported in October 2009 that CBP had made limited progress in scanning containers at the initial ports participating in the Secure Freight Initiative program, leaving the feasibility of 100 percent scanning largely unproven. CBP had not developed a plan for full implementation of a statutory requirement that 100 percent of U.S.-bound container cargo be scanned by 2012.[1] Among other things, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning of all U.S.-bound cargo containers in light of the challenges faced at the initial Secure Freight Initiative ports. DHS concurred with our recommendations. Although DHS has not conducted a feasibility analysis, DHS reported that it is examining alternatives to 100 percent scanning as part of the current effort to develop the National Strategy for Global Supply Chain Security, which is intended to articulate an integrated U.S. government vision for collaborating broadly to manage the risks presented by and to the global supply chain. According to DHS, this strategy is undergoing interagency review, and should be issued in the fall of 2011. This strategy should help DHS more fully evaluate various alternatives for implementing the 100 percent scanning requirement or other alternatives that enhance cargo container security in a cost-efficient manner. However, since the strategy is not yet complete, it is too early to assess its impact.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00826 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.452

[a] Maritime Security and Response Operations requirements were referred to Operation Neptune Shield requirements until November 2010. They require Coast Guard units to escort a certain percentage of high capacity passenger vessels at each maritime security threat level to protect against an external threat, such as a waterborne improvised explosive device. This requirement is applicable to all types of high capacity passenger vessels—cruise ships, ferries, and excursion vessels—in a sector's area of responsibility.

[b] We are conducting our work for the Senate Committees on Commerce, Science and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and the House Homeland Security Committee, Subcommittee on Border and Maritime Security.

[c] The Maritime Transportation Security Act of 2002, as amended, establishes requirements for various layers of maritime security, including requiring a national maritime transportation security plan, area maritime transportation security plans, and facility and vessel security plans. The act calls for various types of facilities to develop and implement security plans, and it places federal responsibility for approving and overseeing these plans with DHS. See Pub. L. No. 107-295, § 102(a), 116 Stat. 2064, 2068 (2002) (codified as amended at 46 U.S.C. § 70103). DHS has placed lead responsibility for this and other Maritime Transportation Security Act requirements with the U.S. Coast Guard. Subsequent Coast Guard guidance called for conducting annual on-site inspections and annual unannounced spot checks to verify a facility's compliance with its security plan.

[d] We are conducting our work for the House Committee on Homeland Security and its Subcommittee on Oversight, Investigations and Management; the House Committee on Energy and Commerce; the House Committee on Transportation and Infrastructure; the Senate Committee on Commerce, Science and Transportation; the Senate Committee on Homeland Security and Governmental Affairs; and Representative Edward Markey.

[e] See Pub. L. No. 109-347, § 108(a), 120 Stat. 1884, 1892 (2006) (codified as amended at 46 U.S.C. § 70107A).

[f] We are conducting this work for the Senate Committee on Commerce, Science, and Transportation; the House Committee on Transportation and Infrastructure; and the Senate Committee on Homeland Security and Governmental Affairs.

[g] The International Maritime Organization is the international body responsible for improving maritime safety. The organization primarily regulates maritime safety and security through the *International Convention for the Safety of Life at Sea, 1974*. In 2006, amendments to this treaty were adopted that mandated the creation of an international long-range identification and tracking system that, in general, requires the International Maritime Organization member state vessels on international voyages to transmit certain information; the creation of data centers that will, among other roles, receive long-range identification and tracking system information from the vessels; and an information exchange network, centered on an international data exchange for receiving and transmitting long-range identification and tracking information to authorized nations.

[h] The National Ocean Policy is policy adopted by executive order that includes a set of overarching guiding principles for management decisions and actions toward U.S. oceans, coasts and the Great Lakes. Exec. Order No. 13,547, 75 Fed. Reg. 43,023 (July 19, 2010).

[i] DNDO announced the termination of the Cargo Advanced Automated Radiography System program in September 2010.

[j] See Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007) (amending 6 U.S.C. § 982(b)).

GAO Contact

For additional information about this area, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00827 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.453

Appendix IX: Immigration Enforcement

What This Area Includes

The Department of Homeland Security (DHS) is responsible for enforcing U.S. immigration and customs laws, and within DHS, U.S. Immigration and Customs Enforcement (ICE) is primarily responsible for immigration and customs enforcement efforts. ICE's key responsibilities and efforts within immigration enforcement include (1) investigating and taking action to address individuals who have committed immigration and customs offenses, such as overstays;[1] addressing immigration law violations at the workplace; investigating human trafficking and smuggling operations; and combating illicit smuggling of firearms, narcotics, and illicit proceeds; and (2) identifying, detaining, and removing aliens subject to removal.[2] As the primary component responsible for immigration and customs enforcement, for fiscal year 2011 ICE had about 20,000 personnel, and its budget authority was about $5.8 billion.[3] Immigration enforcement falls primarily within the Quadrennial Homeland Security Review Mission 3: Enforcing and Administering Our Immigration Laws.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported, and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to immigration enforcement also include the management and training of immigration enforcement human capital, we are not reporting on DHS's progress in this area. Additionally, ICE's customs enforcement efforts include investigations of such offenses as money laundering and other financial crimes. Specifically, ICE reports efforts to address money laundering, including coordinating with federal, state, local, and foreign law enforcement to conduct multi-jurisdictional

[1] Overstays are unauthorized immigrants in the United States who entered the country legally on a temporary basis but then overstayed their authorized periods of admission.

[2] While ICE's immigration enforcement efforts reported by us and the DHS IG primarily fall within Mission 3 of the Quadrennial Homeland Security Review, according to ICE, its efforts to investigate alien smuggling and firearms trafficking fall within Mission 2: Securing and Managing Our Borders as this mission includes disrupting and dismantling transnational criminal and terrorist organizations that smuggle or traffic people, illicit goods, or the proceeds of crime across United States borders, and commit violent acts. For the purposes of this report, we discussed ICE's alien smuggling and firearms trafficking enforcement efforts under the immigration enforcement functional area aligned under QHSR Mission 3, as discussed in appendix I on our scope and methodology.

[3] Although this appendix focuses primarily on enforcement of immigration laws, the resource amounts provided here encompass all ICE mission areas, including enforcement of customs laws.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00828 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.454

criminal investigations targeting organizations involved in the movement and smuggling of illicit proceeds. ICE also reported developing, in collaboration with Mexico, a study of the processes and methods used by transnational criminal organizations to move illicit money from the United States into other countries. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS, particularly ICE, expanded its immigration and customs enforcement programs and activities in key areas on which we have reported, such as overstay enforcement, compliance with workplace immigration laws, alien smuggling, and firearms trafficking. For example, ICE increased its resources for investigating overstays and alien smuggling operations, and deployed border enforcement task forces to investigate illicit smuggling of people and goods, including firearms. In addition, DHS took action to improve the E-Verify program, which provides employers a voluntary tool for verifying an employee's authorization to work in the United States. Specifically, in April 2011 we reported that DHS increased the E-Verify program's accuracy by expanding the number of databases it can query, took actions to safeguard the privacy of personal information for employees who are processed through E-Verify, and implemented steps to prepare for possible mandatory implementation of E-Verify for all employers nationwide. ICE also expanded its programs for identifying and removing aliens from the United States to include, for example, entering into agreements with state and local jurisdictions to assist in identifying aliens subject to removal. However, our work has shown that work remains in these areas. For example, ICE took action to address a small portion of the estimated overstay population in the United States, and lacks measures for assessing its progress in addressing overstays. Moreover, ICE should better leverage opportunities to strengthen its alien smuggling enforcement efforts by assessing the possible use of various investigative techniques, and CBP should better assess progress made in achieving its alien smuggling-related program objectives. We have also reported on weaknesses with the E-Verify program, including challenges in accurately estimating E-Verify costs that put DHS at an increased risk of not making informed investment decisions and developing justifiable budget requests for future E-Verify use and potential mandatory implementation of it. Table 13 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00829 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.455

Table 13: Assessment of Progress and Work Remaining in Key Immigration Enforcement Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Investigations of immigration and customs offenses	DHS dedicated additional resources to overstay enforcement and alien smuggling investigations, and took action to strengthen its voluntary program for helping employers' compliance with immigration laws at the workplace and to combat firearms trafficking. However, DHS lacks measures for assessing the effectiveness of its efforts and should strengthen its investigations by assessing the use of additional investigative techniques, and better ensure that it makes informed investment decisions by developing more reliable cost estimates.	**ICE investigates few overstays, and its efforts should be strengthened by improved planning and performance management.** **Key progress:** ICE took action to address a small portion of the estimated overstay population due to, among other things, competing priorities. In April 2011 we reported that ICE's Counterterrorism and Criminal Exploitation Unit (CTCEU)—the primary federal entity responsible for taking enforcement action to address overstays—prioritizes and assigns overstay cases to field offices for investigation. CTCEU prioritizes in-country overstay leads based on various factors that consider the potential risks overstays may pose to national security and public safety, and field offices investigate those leads that CTCEU identifies as a priority. We reported that field offices had closed about 34,700 overstay investigations that CTCEU headquarters assigned to them from fiscal year 2004 through 2010, as of October 2010. These cases resulted in approximately 8,100 arrests, relative to a total estimated overstay population of 4 million to 5.5 million.[a] Additionally, we reported that since fiscal year 2006, ICE allocated about 3 percent of its investigative work hours to overstay investigations, but was considering assigning some responsibility for noncriminal overstay enforcement to its Enforcement and Removal Operations directorate to expand its overstay enforcement efforts. **What remains to be done:** In April 2011 we reported that ICE lacked measures for assessing its performance in investigating overstays and the quality of its overstay leads sent to field offices for investigation, making it difficult for ICE management to assess program performance and make decisions for program improvements. Among other things, we recommended that ICE establish a time frame for completing overstay enforcement planning and develop measures for assessing the performance and progress of its overstay enforcement efforts. ICE concurred with these recommendations and reported that it planned to take action to address them, such as working with national security partners to determine possible performance measures. In August 2011, ICE reported that it had efforts underway to develop qualitative and quantitative measures related to lead quality, cost effectiveness, process efficiency, and risk, and plans to implement the measures in fiscal year 2012. ICE further reported that it had initiated new targeting methods intended to better ensure it targets leads that pose the greatest security and public safety risks. While these are positive steps, ICE is in the early stages of implementing them and thus, it is too early to assess their effectiveness.
		DHS took steps to improve compliance with immigration laws at the workplace, but a key tool for verifying work eligibility is vulnerable to inconsistent recording of information and unreliable cost estimates. **Key progress:** DHS has taken action to improve the E-Verify program, which provides employers a voluntary tool for verifying an employee's authorization to work in the United States. Specifically, in April 2011 we reported that DHS increased the E-Verify program's accuracy by expanding the number of databases it can query, took actions to safeguard the privacy of personal information for employees who are processed through E-Verify, and implemented steps to prepare for possible mandatory implementation of E-Verify for all employers nationwide. Moreover, in July 2011, DHS reported additional improvements to E-Verify, including initiatives to reduce identity fraud, such as launching a pilot program in one state that will allow E-Verify to confirm the validity and authenticity of driver's licenses used by employees.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00830 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.456

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We reported that the E-Verify program continues to face challenges. For example, we reported that the accuracy of E-Verify is limited by inconsistent recording of employees' names and fraud, and that, because of challenges in accurately estimating E-Verify costs, DHS is at an increased risk of not making informed investment decisions, understanding system affordability, and developing justifiable budget requests for future E-Verify use and potential mandatory implementation of it. Among other things, we recommended that DHS disseminate information to employees on the importance of consistently recording their names, and that DHS ensure that a life cycle cost estimate for E-verify is developed in a manner that reflects the characteristics of a reliable estimate—comprehensive, well-documented, accurate and credible. DHS concurred with these recommendations and reported taking steps toward addressing them, such as disseminating information through various media—guides, websites, videos, and a toll-free employee hotline—to emphasize the importance of recording employees' names consistently and to respond to employee issues. In July 2011, DHS also reported that it was in the final stages of finalizing a life-cycle cost estimate for the program. As DHS is in the early stages of implementing these efforts and has not yet completed its cost estimate, it is too early to assess their impact.
		DHS expanded alien smuggling resources, but should better leverage program resources. **Key progress:** DHS increased its resources for investigating and interdicting alien smuggling activities. In May 2010 we reported that U.S. Customs and Border Protection (CBP) is responsible for interdicting smuggled aliens as illegal border-crossing attempts are made between the ports of entry.[b] CBP maintains several programs that address alien smuggling and collaborates with ICE in providing information for alien smuggling investigations obtained during interdictions. We also reported that ICE work years spent investigating alien smuggling increased from 190 to 197 from fiscal years 2005 through 2009. Furthermore, in May 2010 we reported that ICE and CBP had established objectives for their alien smuggling related enforcement programs, such as objectives to remove aliens who are apprehended during the dangerous summer months to deter them from returning in order to reduce loss of life and disrupt alien smuggling operations.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00831 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.457

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: We reported that ICE and CBP had opportunities to improve efforts to address alien smuggling. Specifically, we reported that ICE should better leverage resources for its alien smuggling investigative efforts by, among other things, assessing the (1) possible expansion of a program for handling state and local law enforcement referrals, including smuggling cases, to help ICE direct more resources toward alien smuggling investigations; and (2) possible use of investigative techniques to follow cash transactions flowing through money transmitters that serve as the primary method of payment to those individuals responsible for smuggling aliens. We also reported that CBP should improve its efforts by better evaluating its progress in meeting its alien smuggling objectives. We recommended, among other things, that DHS evaluate the feasibility of expanding the ICE response program, assess investigative strategies, and establish a plan, including performance measures, for evaluating alien smuggling related enforcement programs. DHS generally concurred with these recommendations and reported actions planned or underway to implement them. For example, in July 2011 CBP reported developing draft performance measures for its alien smuggling-related enforcement programs that are awaiting approval from CBP management. In addition, ICE reported studying the feasibility of expanding the response program and possible use of financial investigative techniques; however, ICE stated that expansion of the program is contingent upon fiscal year 2012 budget decisions. These are positive steps that should strengthen ICE and CBP efforts to address alien smuggling. However, since these efforts are not yet complete, we have not assessed their impact.
		ICE took action to implement its firearms trafficking responsibilities. **Key progress:** In June 2009, we reported that ICE developed its Border Enforcement Security Task Force initiative to help facilitate cooperation and bring together resources of ICE, CBP, and other United States and Mexican law enforcement entities to focus investigative, interdiction, and intelligence assets towards the identification, prioritization, and investigation of emerging or existing threats to our border, such as the investigation of illicit smuggling of people and goods, including firearms. In July 2011, ICE reported various initiatives to further increase interaction and collaboration with its law enforcement partners, such as assigning an analyst to the El Paso intelligence center, which serves as a central repository for weapons-related intelligence information; increasing the number of personnel assigned to Border Enforcement Security Task Forces; and establishing a virtual task force through which United States and Mexican law enforcement can share information regarding weapon seizures.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00832 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.458

Area	Overall assessment	Summary of key progress and work remaining
		We also reported on challenges with ICE's firearms trafficking efforts, which ICE addressed. For example, we reported that ICE could help enhance interagency collaboration in combating arms trafficking to Mexico.[c] Specifically, we found that ICE and the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—the primary agencies implementing efforts to address illicit sales of firearms—did not effectively coordinate their efforts, in part, because the agencies lacked clear roles and responsibilities and had been operating under an outdated interagency agreement, resulting in instances of duplicate initiatives and confusion during operations. Additionally, ICE, along with other agencies, had not systematically gathered, analyzed, and reported data that could be useful to better understand the nature of the firearms trafficking problem, help plan ways to address it, and assess progress made, hampering the investigative capacity of the law enforcement agencies involved. Among other things, we recommended that DHS work with the Department of Justice to finalize the memorandum of understanding they were working on between ICE and ATF. We also recommended that ICE and ATF develop processes for periodically monitoring implementation of the memorandum's provisions so as to make any necessary adjustments and ensure the systematic gathering and reporting of data related to results of enforcement efforts, including firearms seizures, investigations, and prosecutions. DHS agreed with our recommendations and has taken actions and has others underway that should address them. For example, in June 2009 ICE and ATF signed a memorandum of understanding to, in part, formalize their partnership and coordinate collective law enforcement efforts. In addition, ICE developed a system to help ensure oversight and determine whether changes are needed to implement the memorandum. ICE also reported planning to enhance its databases to better capture and track data on enforcement efforts.
Identification, detention, and removal of aliens subject to removal	ICE expanded its programs to identify and remove incarcerated aliens who are eligible for removal.	**ICE expanded its programs and activities to identify and remove criminal aliens in federal, state, and local custody who are eligible for removal from the United States.** **Key progress:** In January 2009 we reported that through ICE's 287(g) program—in which ICE enters into agreements with state and local law enforcement agencies to train officers to assist in identifying those individuals who are in the United States illegally—ICE reported enrolling 67 state and local law enforcement agencies and training 951 state and local law enforcement officers.[d] According to data provided by ICE for 25 of the 29 program participants we reviewed, during fiscal year 2008, about 43,000 aliens had been arrested pursuant to the program.[e] We also reported that ICE had designed some management controls for the 287(g) program, such as memorandums of agreement to govern program implementation and background checks for state and local law enforcement officers. Furthermore, in April 2011, ICE established its 287(g) Communications Plan to provide clear and consistent information about the 287(g) program including the program's goals and policies, among other things. In March and September 2010, the DHS IG reported, in part, that ICE and state and local law enforcement agencies had not complied with all terms of the 287(g) agreements, and the program's performance measures did not always align with program priorities.[f] Similarly, in January 2009 we reported that although ICE had established some management controls for the 287(g) program, it lacked other controls such as documented program objectives to help ensure that participants work toward a consistent purpose. We also reported that ICE lacked performance measures to fully evaluate the 287(g) program, making it difficult for ICE to ensure that the program was operating as intended.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00833 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.459

Area	Overall assessment	Summary of key progress and work remaining
		We and the DHS IG made a number of recommendations to ICE to help address these challenges, which DHS has worked to address. For example, DHS specified in its memorandum of agreement with state and local law enforcement the data that each agency is expected to collect regarding their implementation of the 287(g) program so that ICE can better ensure it has information with which to gauge program results. ICE also put into place controls for the program. Moreover, in May 2011 DHS established performance measures in its 287(g) Strategic Plan for fiscal years 2011-2016, and detailed the process for 287(g) jurisdictions to collect performance data in its Program Performance Measures Guide.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] According to our April 2011 report, the most recent estimates from the Pew Hispanic Center approximated that, in 2006, out of an unauthorized resident alien population of 11.5 million to 12 million in the United States, about 4 million to 5.5 million were overstays. Pew Hispanic Center, *Modes of Entry for the Unauthorized Migrant Population* (Washington, D.C.: May 22, 2006).

[b] Ports of entry are government-designated locations where CBP inspects persons and goods to determine whether they may be lawfully admitted into the country. A land port of entry may have more than one border crossing point where CBP inspects travelers for admissibility into the United States.

[c] Agencies with programs related to arms trafficking include, but are not limited to, DHS's ICE and CBP; the Department of Justice's Bureau of Alcohol, Tobacco, Firearms and Explosives, Drug Enforcement Administration, and the Executive Office for U.S. Attorneys; the Department of State; and the Office of National Drug Control Policy.

[d] The program is named after section 287(g) of the Immigration and Nationality Act, which authorizes the agreements with state and local law enforcement agencies and is codified at 8 U.S.C. §1357(g).

[e] In August 2011, ICE reported a revised estimate of about 46,000 aliens being arrested pursuant to the program in fiscal year 2008.

[f] According to the 287(g) agreement, state and local law enforcement agencies are to identify and initiate removal of criminal aliens based on ICE's top priorities. Specifically, the 287(g) agreement identifies three categories of aliens that are a priority for arrest and detention. The highest priority, Level 1, consists of aliens who have been convicted of or arrested for major drug or violent offenses. Level 2 includes aliens who have been convicted of or arrested for minor drug or property offenses. Level 3 includes aliens who have been convicted of or arrested for other offenses.

GAO Contact

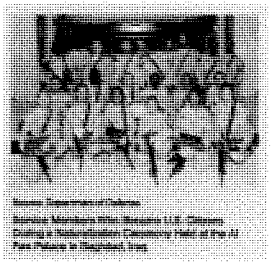
For additional information about this area, contact Richard M. Stana at (202) 512-8816 or stanar@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00834 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.460

Appendix X: Immigration Services

What This Area Includes



Within the Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is the agency primarily responsible for providing immigration services in the United States and internationally at U.S. embassies, consulates and refugee centers. USCIS's key responsibilities and efforts within immigration services include:

- administering immigration benefits, such as processing millions of applications and petitions received each year for about 50 types of immigration benefits for persons seeking to study, work, visit, or live in the United States, and to become U.S. citizens; and
- detecting and resolving suspicious information about and reviewing evidence provided by benefits applicants and petitioners and referring them for fraud investigation and possible sanctioning by other DHS components or external agencies, as appropriate.

As the primary component responsible for immigration services, for fiscal year 2011 USCIS had about 12,000 personnel, and its budget authority was about $2.6 billion. Immigration enforcement falls primarily within the Quadrennial Homeland Security Review Mission 3: Enforcing and Administering Our Immigration Laws.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to immigration services also include immigrant integration, we have not reported on DHS's progress and work remaining in this area. According to USCIS documentation provided to us in July 2011, the agency has undertaken initiatives to support immigrant integration, particularly related to citizenship, including, among other things, outreach, grants for education programs, and improved tools and resources on the citizenship and naturalization process. We currently have work underway for the House Committee on Homeland Security assessing USCIS's immigrant integration efforts, and plan to report on the results of our work later this year.

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS, particularly USCIS, improved the quality and efficiency of the immigration benefit administration process, and strengthened its immigration fraud detection and deterrence efforts. For example, USCIS initiated efforts to modernize its immigration benefit administration infrastructure; improve the efficiency and timeliness of its

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00835 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.461

application intake process; and ensure quality in its benefit adjudication processes. In September 2008 we reported that the USCIS Asylum Division designed training programs and quality reviews to help ensure the integrity of asylum adjudications. In addition, in 2004 DHS established the Office of Fraud Detection and National Security, now a directorate, to lead immigration fraud detection and deterrence efforts, and this directorate has since developed and implemented strategies for this purpose.[1] Further, in July 2011, USCIS reported that it completed the development of a database for analyzing fraud—the Fraud Detection and National Security Data System—which it uses to collect data on fraud and national security concerns. In addition, among other things, USCIS implemented the Administrative Site Visit and Verification Program, through which it conducts pre-and post-adjudication site visit inspections to verify information contained in certain visa petitions.

However, our work and that of the DHS IG have shown that work remains in these areas. For example, USCIS's program for transforming its immigration benefit processing infrastructure and business practices from paper-based to digital systems missed its planned milestones by more than 2 years, and has been hampered by management challenges, such as insufficient planning and not preparing key DHS acquisition planning documents before selecting a contractor to obtain the capabilities needed to transition to an electronic adjudication process. USCIS should also take additional action to address vulnerabilities identified in its assessments intended to determine the extent and nature of fraud in certain applications. Further, in September 2008 we reported that, despite mechanisms USCIS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers cited challenges in identifying fraud as a key factor affecting their adjudications. Table 14 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

[1]The Fraud Detection and National Security Directorate was originally established as an office within the USCIS. In January 2010, the USCIS director elevated the office to directorate level in order to bring greater focus to USCIS's anti-fraud and national security responsibilities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00836 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.462

Table 14: Assessment of Progress and Work Remaining in Key Immigration Services Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Administration of immigration benefits	USCIS initiated efforts to improve the quality and efficiency of its administration of immigration benefits by, among other things, working to transition to an electronic process. However, these efforts have been hampered by management challenges, such as insufficient planning. In addition, preliminary observations from our ongoing work assessing USCIS transformation efforts indicate that USCIS has missed its planned milestones by more than 2 years, and has not adhered to DHS acquisition rules, including not preparing key acquisition planning documents before selecting a contractor to obtain the capabilities needed to transition to an electronic adjudication process.	**USCIS has efforts underway to modernize its benefit administration processes, but these efforts have been hampered by challenges in planning, and preliminary observations from our ongoing work indicate that USCIS has not adhered to DHS acquisition rules.** **Key progress:** Through its transformation initiatives, USCIS aims to upgrade its current, paper-based data systems, which are fragmented, expensive to handle, and prone to handling errors, into a digital processing resource to enhance customer service, improve efficiency with expanded electronic filing, and prevent future backlogs of immigration benefit applications. In July 2007, we reported that USCIS was in the early stages of its Transformation Program and that it had drafted a strategic plan to guide its modernization efforts and established a Transformation Program Office to oversee and carry out the effort. We reported that USCIS's plans partially or fully addressed most key practices for organizational transformations (e.g., by establishing a mission, vision, and integrated strategic goals). **What remains to be done:** In July 2007, we identified challenges in USCIS's transformation plans that created risks that could undermine its success. For example, we reported that the lack of clear and measurable performance measures and targets for the transformed agency put it at risk of developing or selecting new business processes and systems and services that would not achieve the goals of the transformation. Subsequently, in July 2009, the DHS IG found that USCIS positioned itself to better plan and prepare for the next phase in the agency's transformation, including establishing a strategy for deploying the transformed business capabilities and implementing the transformation program. USCIS also implemented pilot programs to test the viability of a number of system capabilities required for the transformation. However, the DHS IG also reported that the success of these pilots had been restricted by factors such as ineffective planning and limited evaluation. Among other things, we recommended that USCIS document specific outcome-oriented performance measures that are aligned with its goals, and the DHS IG recommended that USCIS complete evaluations to document the results and lessons learned from the pilots.[a] USCIS generally concurred with these recommendations and took action to address some and is in the process of addressing others. For example, in July 2010, USCIS reported that it had approved four performance measures that align with its transformation goals, and in July 2011 it reported that it was in the process of developing associated targets for these measures as well as interim measures to gauge usage, customer service, accuracy, and timeliness throughout deployment of the transformed system. In addition, USCIS documented lessons learned from the pilots and stated that it planned to document lessons learned from all future pilots.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00837 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.463

Area	Overall assessment	Summary of key progress and work remaining
		We currently have work underway evaluating USCIS's efforts to implement the Transformation Program.[b] Our preliminary observations indicate that UCSIS has not consistently adhered to DHS acquisition guidance. For example, USCIS did not prepare key acquisition planning documents before selecting a contractor to obtain the capabilities needed to transition to an electronic adjudication process. USCIS does not agree that the agency did not consistently adhere to DHS acquisition guidance because the agency asserts that it produced all documents called for by the guidance. While we agree that USCIS eventually produced the documents, it did not do so before contracting to obtain the needed capabilities as directed by the guidance, and therefore, did not adhere to the guidance. In addition, scheduled deployment of the program's new electronic immigration system is over 2 years behind schedule and by the end of September 2011, USCIS estimates it will have spent about $770 million since the program began in 2006. According to USCIS, the program's delays can be attributed to changes in departmental acquisition policies and a December 2009 decision to modify the planned sequence of deliverables, among other things. USCIS also reported that DHS slowed the program's overall schedule to enhance oversight and better mitigate program risks. Moving forward, improved acquisition planning, including having reliable program schedules, could help USCIS avoid further delays and potential cost overruns. We plan to report on the final results of this review later this year.
		DHS took steps to ensure quality in its application adjudication processes, but encountered challenges, particularly with regard to training. **Key progress:** In February 2008, we reported that the USCIS Humanitarian Affairs Branch designed internal controls to help ensure that requests for humanitarian parole were decided in accordance with applicable guidelines, such as clear and detailed written policies and procedures.[c] However, we also reported that the USCIS Humanitarian Affairs Branch did not have a training program for new staff and staff who may be detailed to process applications, which was essential to ensure that criteria for granting and denying parole were applied consistently and fairly by the adjudicators.[d] We recommended that USCIS develop a training program curriculum on adjudication of humanitarian parole cases for new and detailed staff. In response to our recommendation, USCIS developed a training program and standardized training materials for adjudicating humanitarian parole cases, which it reported implementing in February 2009. Further, in September 2008 we reported that the USCIS Asylum Division had designed training programs and quality reviews to help ensure the integrity of asylum adjudications, such as centralized training for officers that addressed most facets of the asylum adjudication process. In addition to these efforts, in July 2011, USCIS provided us with information on other programs and efforts it has underway to help strengthen its administration of immigration benefits. For example, to help prevent future immigration benefit application backlogs from accruing, USCIS reported that it had developed a tool to identify USCIS offices with additional capacity to adjudicate benefits applications. USCIS indicated that it could shift work from offices with backlogs to offices with additional capacity when needed. USCIS also has developed a forecasting model that projects application receipts to help USCIS anticipate and plan for seasonal application surges. We have not completed work in these areas upon which to make an assessment of USCIS's progress.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00838 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.464

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: In September 2008 we reported that the USCIS Asylum Division lacked key information for making training decisions because it did not consistently solicit input from asylum officers and supervisors on a range of their training needs.[e] We recommended that DHS develop a framework for soliciting information on asylum adjudicators' training needs. DHS concurred with our recommendation and has actions underway to address it. For example, USCIS developed an online training needs assessment that was completed by asylum officers and supervisors between July and August 2010. In July 2011, USCIS reported that it had used the results of the assessment to identify training needs at the national and local levels, and based on these needs, has begun to deploy local training initiatives. While these are positive steps, DHS is in the process of deploying these local training initiatives, and thus, it is too early to assess their results. As we previously reported, supplementing existing training should improve asylum officers' ability to elicit needed information during an applicant interview to help distinguish between a genuine and fraudulent claim.
Immigration benefit fraud	DHS implemented programs and activities for detecting and deterring immigration fraud, but work remains to improve their impact, such as assisting adjudication officers with improving their ability to identify fraud and addressing vulnerabilities identified through USCIS fraud assessments.	**DHS implemented programs and activities for detecting and deterring immigration fraud, but work remains to improve their impact, such as assisting adjudication officers with improving their ability to identify fraud and addressing vulnerabilities identified through USCIS fraud assessments.** **Key progress:** DHS implemented programs for resolving issues related to immigration petitions and applications with potential immigration benefit fraud indicators.[f] In April 2008, the DHS IG reported that the USCIS Fraud Detection and National Security Directorate had identified general strategies for (1) obtaining from adjudicators all petitions with fraud indicators, or articulable fraud, and referring them to U.S. Immigration and Customs Enforcement (ICE) for review; (2) developing a database to enhance the office's ability to analyze fraud; (3) tracking all petitions with articulable fraud indicators from referral to completion; and (4) identifying and analyzing fraud patterns and trends using data mining and pattern recognition to search new immigration petitions against known fraud indicators.[g] In July 2011, USCIS reported that it had completed the development of a database for analyzing fraud—the Fraud Detection and National Security Data System—and uses this system to collect data on fraud and national security concerns. In addition, USCIS reported taking additional steps to enhance its fraud detection and deterrence efforts. These included placing Fraud Detection and National Security Immigration Officers in domestic USCIS offices and in three overseas locations to provide onsite investigations capabilities; developing an intelligence component to share information within and outside of DHS to help develop investigations about individuals who pose a public safety or national security risk; and creating a Threat Assessment Branch to, among other things, provide oversight of fraud detection operations at USCIS centers. USCIS further reported implementing the Administrative Site Visit and Verification Program, through which it conducts pre-and post-adjudication site visit inspections to verify information contained in certain visa petitions, and implementing the Validation Instrument for Business Enterprises Program, through which it uses a Web-based instrument to validate basic information about companies or organizations petitioning to employ alien workers. We have not completed work in these areas upon which to make an assessment of USCIS's progress.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00839 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.465

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: In December 2008 we reported that USCIS needed to take actions to address vulnerabilities in its process for granting permanent residency. For example, USCIS worked to address vulnerabilities identified in two of its assessments intended to determine the extent and nature of fraud in certain application types that may lead to permanent residency, such as increasing site visits and requirements to verify the legitimacy of institutions petitioning for benefits for religious workers. However, USCIS had not released reports on three other benefit fraud and compliance assessments and had not completed actions to address vulnerabilities identified in four assessments. These assessments indicated, for example, that some asylum applicants submitted false arrest and medical reports to support their claims of persecution, and some such fraudulent applications had been approved by USCIS adjudicators. We concluded that the vulnerabilities identified by these assessments, such as failure to verify the evidence applicants and their petitioners provide, would persist until USCIS took corrective actions, thereby increasing the risk that ineligible individuals would obtain lawful permanent resident status. Further, in September 2008 we reported that, despite mechanisms USCIS had designed to help asylum officers assess the authenticity of asylum claims, such as identity and security checks and fraud prevention teams, asylum officers cited challenges in identifying fraud as a key factor affecting their adjudications. For example, 73 percent of asylum officer survey respondents reported it was moderately or very difficult to identify document fraud. We also found that assistance from other federal entities to asylum officers in assessing the authenticity of asylum claims had been hindered in part by resource limitations and competing priorities. We recommended that, among other things, USCIS prepare a roadmap for each of the four outstanding benefit fraud and compliance assessments that delineates timetables for deciding what actions to take, which USCIS organizational units will be responsible for implementing, and a timetable for implementing agreed-upon actions. We also recommended that, in order to help asylum officers refine their interview techniques to elicit information to use in assessing credibility, determining eligibility, and distinguishing between genuine and fraudulent claims, the Asylum Division explore ways to provide additional opportunities for asylum officers to observe skilled interviewers. DHS agreed with these recommendations, has addressed some, and has actions underway to address others. For example, USCIS developed a draft plan for asylum officer interview observation opportunities to occur quarterly, and reported in July 2011 that it was continuing to explore different models for interview observations. In addition, in July 2011, USCIS reported that it had established a Fraud Detection and National Security component within the Refugee, Asylum, and International Operations Directorate in order to improve fraud detection and prevention capabilities across the directorate, which includes the Asylum Division. With respect to addressing vulnerabilities identified in its outstanding benefit fraud and compliance assessments, in August 2011, USCIS officials told us that USCIS was in the process of hiring a contractor to assist with the effort of revising how these assessments were conducted, and that the review and timetable for implementing actions related to the outstanding assessments would depend on the contractor's findings. USCIS further reported that the procurement for the contractor was underway. Once the assessments are reviewed, USCIS expects to begin implementing our recommendation to develop roadmaps for addressing their findings.

Source: GAO analysis.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00840 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.466

Note: This table also includes examples from selected DHS IG reports.

[a] Outcome-oriented performance measures show results or outcomes related to an initiative or program in terms of its effectiveness, efficiency, or impact.

[b] We are conducting this work for the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on the Judiciary, and the Senate Committee on the Judiciary.

[c] The Humanitarian Affairs Branch was formerly called the Humanitarian Assistance Branch.

[d] Aliens who are otherwise inadmissible but have an urgent humanitarian need may apply to USCIS's Humanitarian Affairs Branch for humanitarian parole, which permits an alien to enter the United States on a temporary basis.

[e] Each year tens of thousands of noncitizens apply in the United States for asylum, which provides refuge to those who have been persecuted or fear persecution. The Asylum Division within USCIS is responsible for adjudicating these applications.

[f] Benefit fraud might involve a conspiracy in which an organization profits from thousands of fraudulent applications, or what DHS refers to as "single-scope fraud," such as two individuals agreeing privately to a fraudulent marriage.

[g] Articulable fraud encompasses any application with concrete evidence that leads the adjudicator to suspect fraud, such as contradictory statements on material facts, atypical or boilerplate applications, or suspected fraudulent documents. Pursuant to a September 2008 memorandum of agreement between USCIS and ICE, USCIS no longer refers all fraud cases to ICE. Rather, USCIS refers those cases that are most likely to result in criminal investigations to ICE and investigates the remaining cases itself.

GAO Contact

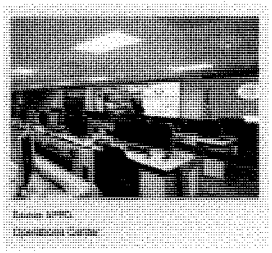
For additional information about this area, contact Richard M. Stana at (202) 512-8816 or stanar@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00841 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.467

Appendix XI: Critical Infrastructure Protection—Cyber Assets

What This Area Includes



The Department of Homeland Security (DHS) has overall responsibility for coordinating critical infrastructure protection efforts for 18 critical infrastructure sectors—such as energy, water, and communications. Within DHS, the National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) is charged with enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CS&C's key responsibilities and efforts related to cybersecurity include (1) risk assessment and planning; (2) protection and resiliency; and (3) partnerships and coordination mechanisms. As the primary DHS component responsible for safeguarding physical and cyber assets, in fiscal year 2011 NPPD, which includes CS&C, had about 2,800 personnel and its budget authority was about $2.3 billion.[1] Critical infrastructure protection of cyber assets primarily falls within the Quadrennial Homeland Security Review Mission 4: Safeguarding and Securing Cyberspace.

In 1997 we designated federal information security as a high-risk area, and in 2003 we expanded this area to include cyber critical infrastructure protection. In designating these issues as high-risk, we reported that federal agencies and our nation's critical infrastructure—such as power distribution, water supply, telecommunications, and emergency services—rely extensively on computerized information systems and electronic data to carry out their operations. The security of these systems and data is essential to protecting national and economic security, and public health and safety. Safeguarding federal computer systems and the systems that support critical infrastructure—referred to as cyber critical infrastructure protection—is a continuing concern. In our January 2009 high-risk update, we reported that federal agencies made progress in strengthening information security, but that most agencies continued to experience significant deficiencies that jeopardize the confidentiality, integrity, and availability of their systems and information. We also reported that DHS, as the focal point for federal efforts to protect the nation's critical infrastructure continued to make progress in fulfilling its key cyber critical infrastructure protection responsibilities. However,

[1] The goal of the NPPD is to advance the Department's risk-reduction mission. CS&C is within NPPD. Other divisions or offices within NPPD include, for example, the Federal Protective Service and the Office of Infrastructure Protection. The NPPD budget authority for fiscal year 2011 includes $1.3 billion in appropriated funds, and the authority to collect another $1.1 billion in fees for the Federal Protective Service. These values do not add up to $2.3 billion due to rounding.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00842 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.468

but in the February 2011 high-risk update we identified several areas of responsibility that required further attention, such as advancing cyber analysis and warning capabilities, acquiring sufficient analytical and technical capabilities, and strengthening the effectiveness of the public-private sector partnerships in securing cyber critical infrastructure. In January 2011, DHS provided us with a corrective action plan for this high-risk area. We provided DHS with feedback on this plan noting, for example, that the plan included objectives, milestones, and planned accomplishments related to DHS's cybersecurity responsibilities. However, we identified aspects of the plan that should be strengthened, such as clarifying whether DHS's 2010 goals and objectives for its corrective actions were met, and identifying resources needed and planned milestones for 2011 activities.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. DHS has other ongoing efforts related to cyber critical infrastructure protection, such as the assessment of cybersecurity measures implemented at high-risk chemical facilities as part of its Chemical Facility Anti-Terrorism Standards program, on which we have not reported. DHS also established the National Cybersecurity and Communications Integration Center in October 2009 to serve as a national cyber and communications operations center to fuse information from federal civilian agencies, law enforcement, intelligence, state and local government, and the private sector. Further, DHS signed a memorandum of agreement with the Department of Defense to improve cyber coordination.[2] In addition, according to DHS officials, NPPD's Office of Infrastructure Protection and the National Cyber Security Division collaborated to integrate cybersecurity elements into the Office of Infrastructure Protection's facility security and vulnerability assessments. The National Cyber Security Division also conducts cyber assessments in support of the Office of Infrastructure Protection's Regional Resiliency Assessment Program and major national events, according to DHS. We have not completed work on these areas upon which to make an assessment of DHS's progress.

[2] The Department of Defense also has responsibilities for cybersecurity efforts.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00843 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.469

Key Progress and Work Remaining

Our work, supplemented by the work of the DHS IG, has shown that DHS expanded its efforts to conduct cybersecurity risk assessments and planning, provide for the protection and resilience of cyber assets, and implement cybersecurity partnerships and coordination mechanisms. For example, DHS updated the *National Infrastructure Protection Plan* to include an emphasis on cybersecurity issues by listing progress made and new initiatives related to cybersecurity. In addition, DHS took steps to secure external network connections in use by the federal government by establishing the National Cybersecurity Protection System, operationally known as Einstein, to analyze computer network traffic information to and from agencies. Additionally, the agency made progress in enhancing its cyber analysis and incident warning capabilities through the establishment of the U.S. Computer Emergency Readiness Team, which, among other things, coordinates the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. DHS is also working to improve cyber-related partnerships with public and private stakeholders by developing new information-sharing arrangements and addressing corrective actions based on a cybersecurity exercise. In September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing lessons it had learned from these efforts to strengthen public and private incident response capabilities.

However, our work and that of the DHS IG has also shown that key challenges remain in these efforts. For example, to expand its protection and resiliency efforts, DHS needs to lead a concerted effort to consolidate and better secure Internet connections at federal agencies. DHS also faces challenges in fully establishing a comprehensive national cyber analysis and warning capability. For example, in July 2008, we reported that the U.S. Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities. Moreover, the DHS IG reported that DHS needs to establish a consolidated, multiple classification level portal that can be accessed by federal partners with real-time incident response related information and reports. Additionally, expectations of private sector stakeholders are not being met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. We also reported that public sector stakeholders believed that improvements could be made by improving private sector sharing of sensitive information. Table 15 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00844 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.470

Table 15: Assessment of Progress and Work Remaining in Key Critical Infrastructure Protection—Cyber Assets Areas on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
Risk assessment and planning	DHS updated the *National Infrastructure Protection Plan* to include an emphasis on cybersecurity issues, including methodologies to identify systems or networks of national significance. In addition, DHS met and worked with lead federal agencies to update sector specific plans with the goal of fully addressing cyber-related requirements. Most agencies updated their respective plans, and it is important that the plans address cybersecurity requirements.	**DHS placed a greater emphasis on cybersecurity issues in the updated *National Infrastructure Protection Plan*, and directed lead federal agencies to address cybersecurity issues in sector specific plans and sector risk assessments. Most agencies updated their respective plans, and it is important for these updated plans to address cybersecurity requirements to provide information on the implementation of cyber-related protective measures.** **Key progress:** DHS included a greater emphasis on cybersecurity in the 2009 *National Infrastructure Protection Plan* than it did in the first iteration of the plan in 2006. The plan provides the overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. In March 2010 we reported that the new 2009 plan lists the progress made and new initiatives related to cybersecurity, including the development of cross-sector cyber methodologies to identify systems or networks of national significance; the addition of a cross-sector cybersecurity working group; and a public-private cross-sector program specifically for cybersecurity. The plan also identified new responsibilities for critical infrastructure partners to conduct cybersecurity exercises to test the security of cyber systems, as well as the development of cybersecurity-specific vulnerability assessments by DHS. In addition, DHS developed the first National Cyber Incident Response Plan in September 2010 to coordinate the response of multiple federal agencies, state and local governments, and hundreds of private firms, to incidents at all levels. Further, following the publication of the 2009 *National Infrastructure Protection Plan*, DHS directed sector specific agencies to give additional attention to cybersecurity when developing their sector specific plans and sector annual reports.[a] These plans provide the means by which the *National Infrastructure Protection Plan* is implemented across the sectors and articulate the progress of the sectors' critical infrastructure protection and resiliency efforts, challenges, and needs respectively. Regarding cybersecurity, the guidance calls for the sector specific agencies to include goals or long-term objectives for cybersecurity in their sector and explain their approach for identifying their sector's cyber assets, systems, networks, and functions; incorporating cyber elements into sector risk assessments; and prioritizing cyber elements—such as communication and computer networks—of the sector, among other things, as appropriate to each sector.[b] **What remains to be done:** In September 2009 we reported that, among other things, sector-specific agencies had not yet updated their respective sector-specific plans to fully address key DHS cybersecurity criteria. In addition, most agencies had not updated the actions and reported progress in implementing them as called for by DHS guidance. We found that of the 17 sector-specific plans, 9 had been updated, of which 3 addressed DHS's cybersecurity criteria. We noted that these shortfalls were evidence that the sector planning process had not been effective and thus left the nation in the position of not knowing its status in securing cyber critical infrastructure.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00845 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.471

Area	Overall assessment	Summary of key progress and work remaining
		We recommended that DHS (1) assess whether existing sector-specific planning processes should continue to be the nation's approach to securing cyber and other critical infrastructure, and consider whether other options would provide more effective results; and (2) collaborate with the sectors to develop plans that fully address cybersecurity requirements. DHS concurred and reported, for example, that it worked with sector officials to update sector plans with the goal of fully addressing cyber-related requirements. In 2010, the sectors issued 18 updated plans to be reviewed by federal agencies, such as the Office of Management and Budget and DHS. As of August 2011, DHS officials stated that 17 plans were finalized and 1 was in the process of being reviewed. DHS officials were not able to provide milestones for when the remaining plan would be finalized, as it is under federal interagency review. We have not yet reviewed these plans to determine the extent to which they address specified security requirements. Having plans with complete updates that address cybersecurity requirements will be important in providing the nation with information on where we are in implementing associated protective measures designed to secure and protect the nation's cyber and other critical infrastructure.[c]
Protection and resiliency	DHS took steps to secure external network connections in use by the federal government, and to coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. However, to expand protection and resiliency efforts, concerted effort is needed to consolidate and secure Internet connections at federal agencies. DHS also faces challenges in establishing a comprehensive national cyber analysis and warning capability.	**DHS enhanced the protection and resiliency of federal computer networks, but a concerted effort is needed to consolidate and secure Internet connections at federal agencies.** **Key progress:** To reduce the threat to federal systems and operations posed by cyber attacks on the United States, the Office of Management and Budget launched, in November 2007, the Trusted Internet Connections initiative. In 2008, DHS's National Cybersecurity Protection System, operationally known as Einstein, became mandatory for federal agencies as part of this initiative.[d] In March 2010, we reported on federal agencies' efforts to meet the requirements of the Trusted Internet Connections Initiative, which is directed by the Office of Management and Budget with assistance from DHS.[e] Although agencies were in the process of implementing the initiative, we reported that it was resulting in benefits to agencies including improved security and network management. In 2008, DHS developed Einstein 2, which incorporated network intrusion detection technology into the capabilities of the initial version of the system.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00846 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.472

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: Although we found that agencies reported benefits from the Trusted Internet Connection Initiative, none of the 23 agencies we reviewed met all of the requirements of the Trusted Internet Connections Initiative, as of September 2009.[f] Most agencies reported that they have made progress toward reducing their external connections and implementing critical security capabilities, but they also experienced delays in their implementation efforts.[g] Further, agencies had not demonstrated that they fully implemented the required security capabilities. Agencies had been challenged in implementing the initiative, in part because DHS did not always respond to agency queries on security capabilities in a timely manner. Agencies' experiences with implementing the initiative offered DHS lessons learned, such as the need to define program requirements before establishing deadlines, and the usefulness of sponsoring collaborative meetings for agencies' implementation efforts. In addition, because DHS did not conduct direct testing of the critical security capabilities or evaluate all possible locations in its validation reviews, we concluded that it could not be assured that all critical security capabilities had been implemented. Among other things, we recommended that DHS enhance Trusted Internet Connections' compliance validations by including (1) direct testing and evaluation of the critical capabilities, and (2) evaluation of the capabilities at all agency Trusted Internet Connections locations. DHS concurred with our recommendations and stated that it was taking steps to address them, such as developing and deploying two tools in 2011—one that automates cybersecurity compliance validation, and one that identifies which government owned Internet domains are in compliance with federal guidelines. In July 2011 DHS reported that it conducted assessments that included direct testing of critical security capabilities. However, we have not yet assessed these efforts, as DHS recently conducted this direct testing and is in the process of implementing these two tools. In addition, we reported that DHS had started to deploy Einstein to federal agencies, but faced challenges with meeting program goals. The U.S. Computer Emergency Readiness Team created Einstein in 2003 with the intention to provide DHS with an increased awareness of computer network traffic activity, including possible security incidents, on federal networks by providing intrusion detection capabilities that allow DHS to monitor and analyze agencies' incoming and outgoing Internet traffic. Agencies that participated in Einstein 1 improved identification of incidents and mitigation of attacks. However, as of September 2009, fewer than half of the 23 agencies we reviewed had executed the required agreements with DHS. We identified several challenges that DHS faced regarding deploying Einstein 2, including understanding the extent to which its objective is being met because DHS lacks performance measures for Einstein 2 that address whether agencies report if the alerts represent actual incidents. We also determined that Einstein could fail to fully meet the objective of increasing U.S. Computer Emergency Readiness Team's situational awareness because DHS did not always ensure that key agreements were executed with agencies. We recommended, among other things, that DHS develop additional performance measures that indicate how agencies respond to alerts. DHS concurred and in July 2011 stated that it is taking actions to develop performance measures. As DHS is in the process of developing these measures, it is too early to assess their results. Performance measures will be important in helping DHS understand how agencies respond to alerts.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00847 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.473

Area	Overall assessment	Summary of key progress and work remaining
		In addition, DHS officials stated that the department piloted Einstein 3 (the Comprehensive National Cybersecurity Initiative 3), which is intended to be an intrusion prevention system that is to automatically detect and respond appropriately to cyber threats before harm is done. According to DHS officials, once fully deployed, Einstein 2 and 3 will provide cyber protection capabilities to more than 110 federal civilian executive branch departments and agencies. As of July 2011, DHS reported that Einstein 2 was deployed at 16 of 19 access provider agencies and active at 15 of them, and that it is fully deployed and active at each of the 4 private telecommunications service providers through which non-access provider agencies seek Managed Trusted Internet Protocol Services.[h] Taking steps to expand cyber protection capabilities to additional federal departments and agencies should help to improve the nation's cyber infrastructure if those capabilities are implemented effectively. However, we have not yet assessed the effectiveness of these efforts as DHS is in the process of deploying Einstein 2 and 3.
		With the establishment of the U.S. Computer Emergency Readiness Team, DHS took steps to coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. However, DHS faces challenges in establishing a comprehensive national cyber analysis and warning capability. **Key progress:** When incidents such as data loss or theft, computer intrusions, and privacy breaches occur, agencies are to notify the U.S. Computer Emergency Readiness Team. Over the past 5 years, the number of incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team has increased; from 5,503 incidents in fiscal year 2006 to 41,776 incidents in fiscal year 2010, an increase of over 650 percent. We currently have work underway assessing the adequacy and effectiveness of agency information security policies and practices, and agencies' implementation of the Federal Information Security Management Act of 2002 requirements, and plan to report on our results later this year.[i] **What remains to be done:** In July 2008, we reported that the U.S. Computer Emergency Readiness Team did not fully address 15 key attributes of cyber analysis and warning capabilities. These attributes are related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, the U.S. Computer Emergency Readiness Team provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. We recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability. DHS generally concurred and stated that it is taking steps to implement them, such as opening two 24-hour centers to increase communication channels and organize cyber response efforts.[j] We are currently working with DHS officials to more fully determine the status of their efforts to address these recommendations.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00848 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.474

Area	Overall assessment	Summary of key progress and work remaining
		The DHS IG also identified challenges with the U.S. Computer Emergency Readiness Team analysis and warning program, which DHS took steps to address. In June 2010 the DHS IG reported that the U.S. Computer Emergency Readiness Team made progress in implementing a cybersecurity program to assist federal agencies in protecting their information technology systems against cyber threats. However, the IG reported that the team could further improve its analysis and warning program. For example, the IG reported that the team could improve its management oversight by developing a strategic plan and establishing performance measures. Additionally, the IG reported that the team should improve its information sharing and communications coordination efforts with the public. Several factors have hampered DHS's ability to share information with its partners, including that threat information from intelligence agencies is classified. The DHS IG recommended, among other things, that DHS establish a consolidated, multiple classification level portal that can be accessed by federal partners that includes real-time incident response related information and reports. In addition, the DHS IG recommended the establishment of specific outcome-based performance measures and a strategic plan to ensure that the team can achieve its mission, objectives, and milestones. DHS concurred with these recommendations, and took action to implement them. For example, DHS reported that it established performance measures and a strategic plan, concept of operations, and standard operating procedures for the U.S. Computer Emergency Readiness Team. In July 2011 DHS also reported that it was taking steps to establish a multiple classification level portal.
Partnerships and coordination mechanisms	Federal partners, including DHS, developed new information-sharing arrangements, and DHS completed corrective actions based on a cybersecurity exercise. However, efforts to meet the expectations of private sector stakeholders in areas related to sharing information about cyber-based threats to critical infrastructure should be improved.	**DHS developed new information-sharing arrangements and completed corrective actions based on a cybersecurity exercise. However, additional action is needed to better ensure that expectations of private sector stakeholders are met by their federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.** **Key progress:** DHS completed corrective actions based on lessons learned from a cybersecurity exercise. In September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS demonstrated progress in addressing 8 lessons it had learned from this exercise to strengthen public and private incident response capabilities.[k] In the months following its first exercise, DHS identified 66 activities that address one or more of the lessons, including hosting meetings with key cyber response officials from foreign, federal, and state governments and private industry, and refining their operating procedures. We reported in September 2008 that DHS's actions to address the lessons had not been fully implemented, and consequently recommended that DHS schedule and complete all of the corrective activities identified to strengthen coordination between public and private sector participants in response to significant cyber incidents. As of September 2010, DHS demonstrated that it had completed all 66 of the corrective actions addressing lessons learned from the exercise.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00849 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.475

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: Federal policy, including DHS's *National Infrastructure Protection Plan*, calls for a partnership model that includes public and private councils to coordinate policy and information sharing and analysis centers to gather and disseminate information on threats to physical and cyber-related infrastructure.[l] In July 2010, we reported that while federal partners, such as DHS, were developing new information-sharing arrangements, they were not meeting the key expectations of the private sector. We also reported that public sector stakeholders believed that improvements could be made to the partnership, including improving private sector sharing of sensitive information. We recommended, among other things, that DHS use our findings to focus its information-sharing efforts on the most desired services, including access to sensitive or classified information and a secure mechanism for sharing information. DHS concurred with our recommendations and stated that it took steps to implement them, such as initiating pilot programs to enable the mutual sharing of cybersecurity information at various classification levels.[m] However, as DHS is initiating these pilot programs, it is too early to assess the extent to which they address the challenges we identified.

Source: GAO analysis.

Note: This table also includes examples from selected DHS IG reports.

[a] Sector specific agencies are lead federal agencies for the nation's critical infrastructure sectors, which include, for example, water and energy.

[b] At the time of our review, there were only 17 critical infrastructure sectors. DHS established the 18th sector—critical manufacturing—in March 2008 under the authority of the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.

[c] In addition, DHS reported that in 2009 it released the Information Technology Sector Baseline Risk Assessment and four associated risk management strategies, with it partner entities.

[d] The Trusted Internet Connection initiative is intended to improve security by reducing and consolidating external network access points and by providing centralized monitoring at a select group of access providers, while Einstein is an intrusion detection system that provides an automated process for DHS to analyze computer network traffic information to and from agencies.

[e] All federal agencies in the executive branch, except for the Department of Defense, have been directed to implement the initiative. The goals of the initiative are to secure federal agencies' external network connections, including Internet connections, and improve the government's incident response capability by reducing the number of agencies' external network access points and implementing security controls over the access points that remain.

[f] Under the Trusted Internet Connections initiative federal agencies were required to (1) inventory external connections; (2) establish a target number of Trusted Internet Connections access points; (3) develop and implement plans to reduce their connections; (4) implement security capabilities (if they chose to be an access provider) addressing such issues as encryption and physical security; and (5) demonstrate to DHS the consolidation of connections and compliance with the security capabilities (if they chose to be an access provider).

[g] For example, the 16 agencies that chose to become access providers reported that they had reduced their number of external connections from 3,286 to approximately 1,753.

[h] In implementing the Trusted Internet Connections initiative, agencies could either provide their own access points by becoming an access provider or seek service from these providers or an approved vendor. For agencies seeking service, the agencies obtain services from a multi-service agency or through the Networx program. This program, managed by the General Services Administration, provides an acquisition vehicle for agencies to procure telecommunication, network, wireless, and information technology security services, including Trusted Internet Connections services, from among multiple vendors.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00850 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.476

[i]We are conducting this work in accordance with a mandate in the Federal Information Security Management Act of 2002. Pub. L. No. 107-347, § 301(b), 116 Stat. 2946, 2953 (2002) (codified as amended at 44 U.S.C. § 3545(h)).

[j]According to DHS, in October 2009, it opened the new National Cybersecurity and Communications Integration Center—a 24-hour, DHS-led center to serve as the nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture; and, in November 2010, the Multi-State Information Sharing and Analysis Center, funded in part by DHS, opened the Cyber Security Operations Center, a 24-hour watch and warning facility, to enhance situational awareness at the state and local level and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments.

[k]These lessons involved improving (1) the interagency coordination groups; (2) contingency planning, risk assessment, and roles and responsibilities; (3) integration of incidents across infrastructures; (4) access to information; (5) coordination of response activities; (6) strategic communications and public relations; (7) processes, tools, and technology; and (8) the exercise program.

[l]Information-sharing and analysis centers were established to serve an operational role such as providing mechanisms for gathering, analyzing, and disseminating information on physical and cyber-related infrastructure threats and vulnerabilities to and from private infrastructure sectors and the government.

[m]DHS also reported that it participates in various working groups related to cybersecurity.

GAO Contact

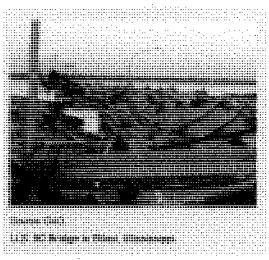
For additional information about this area, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00851 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.477

Appendix XII: Emergency Preparedness and Response

What This Area Includes



The Federal Emergency Management Agency (FEMA), within the Department of Homeland Security (DHS), is the federal agency primarily responsible for emergency preparedness and response efforts. FEMA's key responsibilities and efforts include national emergency preparedness and response planning, such as developing the *National Response Framework* and a national preparedness goal; providing emergency assistance and services, such as temporary housing assistance after a disaster; and supporting the federal government's state, local, and tribal partners' efforts to enhance their emergency management and homeland security capabilities, such as emergency communications, through grants and technical assistance.[1] As the primary component responsible for emergency preparedness and response, in fiscal year 2011 FEMA had approximately 7,300 personnel, and its budget authority was about $10.5 billion.[2] Emergency preparedness and response falls within the Quadrennial Homeland Security Review Mission 5: Ensuring Resilience to Disasters.

For the purposes of this report, we are focusing generally on key areas on which we or the DHS Office of Inspector General (IG) have recently reported and not on areas in which our two agencies have not reported or have conducted limited audit work. For example, while DHS's responsibilities related to emergency preparedness and response also include areas such as human capital management and training and exercise programs, we are not reporting on DHS's progress and work remaining in these areas. With regard to human capital, FEMA reported to us in July 2011 that it planned to increase its staffing levels to enhance FEMA's investigative operations and fraud awareness training initiatives by 50 percent in fiscal year 2011, and by another 50 percent in fiscal year 2012. We have not completed recent work on these areas upon which to make an assessment of DHS's progress.

[1]The National Response Framework is a guide for how the federal, state, local, and tribal governments, along with nongovernmental and private sector entities, will collectively respond to all disasters, ranging from large-scale terrorist attacks or catastrophic disasters such as Hurricane Katrina to serious local incidents, regardless of their cause. The national preparedness goal aims to define the core capabilities necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the United States, and emphasizes actions aimed at achieving an integrated, layered, and all-of-nation preparedness approach that optimizes the use of available resources.

[2] About $5.3 billion of this total was allocated to preparedness, disaster, and other grants, according to FEMA.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00852 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.478

Key Progress and Work Remaining

Our work, supplemented by that of the DHS IG, has shown that FEMA expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; supported state, local, and tribal partners' disaster preparedness and response capabilities; and enhanced emergency communications. For example, FEMA developed various plans for disaster preparedness and response. In particular, FEMA issued the *National Response Framework*, which outlines the guiding principles and major roles and responsibilities of government, nongovernmental organizations, and private sector entities for disaster response. It is also finalizing a National Disaster Recovery Framework, intended to provide a model to identify and address challenges that arise during the disaster recovery process. Moreover, DHS issued the *National Emergency Communications Plan*—the first strategic document for improving emergency communications nationwide. We also reported that FEMA awards certain preparedness grants based on a reasonable risk methodology. However, more work remains in FEMA's efforts to assess capabilities for all-hazards preparedness, provide long-term disaster recovery assistance, and strengthen alert systems. For example, FEMA has faced difficulties in collecting reliable and consistent data and developing measurable target capabilities for national preparedness. Further, with regard to long-term disaster recovery assistance, FEMA's criteria for when to provide the assistance were vague, and, in some cases, FEMA provided assistance before state and local governments had the capacity to work effectively with FEMA. Further, FEMA has faced technical challenges in implementing the Integrated Public Alert and Warning System related to systems integration and alerts for individuals with disabilities, among other things.[3] Additionally, FEMA should improve the efficacy of the grant application and review process by mitigating duplication or redundancy within the agency's various preparedness grant programs. Table 16 provides more detailed information on our assessment of DHS's progress and remaining work in key areas on which we have reported, with an emphasis on work completed since 2008.

[3] The Emergency Alert System is the nation's primary alerting system, proving capacity for the United States to issue alerts and warnings to the public in response to emergencies. The Integrated Public Alert and Warning System is defined by FEMA as a "system of systems," which is intended to integrate existing and new alert systems, including the Emergency Alert System. The Integrated Public Alert and Warning System will supersede the Emergency Alert System as the nation's primary alert function.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00853 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.479

Table 16: Assessment of Progress and Work Remaining in Emergency Preparedness and Response on Which We Have Reported

Area	Overall assessment	Summary of key progress and work remaining
National emergency preparedness and response planning	DHS took steps to improve national emergency preparedness and response planning efforts by releasing the *National Response Framework* and strengthening response and recovery planning. However, a number of operational plans are not yet complete. Further, DHS has not developed measures for assessing national preparedness.	**FEMA issued the *National Response Framework* for disaster preparedness and response, but has not developed or implemented some plans and did not always ensure consistent stakeholder participation in the development and revision of all policies and plans.** **Key progress:** Planning and preparing for a major disaster—particularly a catastrophic disaster that could quickly overwhelm state and local responders—requires the coordinated effort of federal, state, local, and tribal governments, nongovernmental organizations, and the private sector, which owns much of the nation's critical infrastructure. In 2004 DHS issued the *National Response Plan*. In August 2005 Hurricane Katrina revealed a number of limitations in the 2004 *National Response Plan*, and DHS made modifications to it pending a more comprehensive review. DHS completed its revision with the issuance of the *National Response Framework* core document in January 2008, which outlines the guiding principles and major roles and responsibilities of government, nongovernmental organizations, and private sector entities for response to disasters of all sizes and causes. In June 2008 we reported that during the revision process for the *National Response Framework*, DHS did not collaborate with non-federal stakeholders. For example, after the first draft of the *National Response Framework* was completed, DHS limited communication with non-federal stakeholders until it released another draft 5 months later. Further, DHS did not manage the revision process in accordance with the Post-Katrina Emergency Management Reform Act of 2006 provision that DHS establish FEMA's National Advisory Council and incorporate the Council's nonfederal input into the revision because the Council was created after the statutory target date and did not hold its first meeting until the final day of the public comment period for the *National Response Framework* draft.[a] Given that FEMA anticipates the Framework would be revised in the future, in June 2008 we recommended that FEMA develop policies and procedures to guide how future revision processes will occur, particularly for collaborating with nonfederal stakeholders. FEMA concurred and subsequently established provisions that direct the conditions and timing of revisions to the *National Response Framework*.[b] Further, in April 2009, we reported that FEMA had completed most of the key policies, such as the base *National Response Framework*, to define emergency preparedness and response roles and responsibilities. For example, DHS issued the revised National Incident Management System in December 2008 to further clarify roles and responsibilities when multiagency, intergovernmental entities are involved in a response.[c] FEMA also completed key components of the *National Response Framework*, including 15 Emergency Support Function Annexes, and 8 Support Annexes.[d]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00854 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.480

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: In April 2009 we reported that FEMA had not yet completed about two-thirds of the plans to operationalize the policies it had established to define emergency preparedness and response roles and responsibilities. As a result, the roles and responsibilities of key officials involved in responding to a catastrophe had not been fully defined and, thus, could not be tested in exercises. We recommended that FEMA establish a program management plan to ensure that the plans that were called for as part of the national preparedness system were developed in a timely and integrated fashion. FEMA generally concurred and has actions underway to address it. For example, FEMA told us that since we last reported, it has revised or completed six concept plans and approximately 28 hazard-specific regional plans. FEMA also reported working to implement elements of Presidential Policy Directive 8: National Preparedness. This directive instructs the Secretary of Homeland Security to develop a national preparedness goal and national preparedness system to meet that goal through an integrated set of guidance, programs, and processes. Specifically, FEMA reported in August 2011 that in response to Presidential Policy Directive 8, FEMA is leading the development of a Federal Interagency All-Hazards Response Plan, to include scenario-specific annexes that integrate prior earthquake, hurricane, and catastrophic planning efforts. To implement Presidential Policy Directive 8, FEMA will need to review its current and pending policies to ensure that they are consistent with the goals and requirements of the Directive, and make any adjustments that may be needed.
		Despite ongoing efforts to measure preparedness and assess capabilities, FEMA faced difficulties in collecting reliable and consistent data, and developing measurable target capabilities. **Key progress:** DHS, particularly FEMA, implemented efforts to measure preparedness by assessing capabilities and addressing related challenges. In September 2007, DHS issued the National Preparedness Guidelines that describe a national framework for capabilities-based preparedness as a systematic effort that includes sequential steps to first determine capability requirements and then assess current capability levels. As a companion to the Guidelines, FEMA issued a Target Capabilities List, designed to provide a national-level generic model of capabilities defining all-hazards preparedness. FEMA also made progress in developing a system for assessing national preparedness capabilities by, among other things, establishing reporting guidance for state preparedness and issuing a federal preparedness report. Presidential Policy Directive 8, issued in March 2011, requires the development of a national preparedness goal, system, and report. The implementation plan for the directive calls for the development of the national preparedness goal by September 25, 2011, and the development of other documents by September 25, 2012.[e]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00855 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.481

Area	Overall assessment	Summary of key progress and work remaining
		What remains to be done: The success of FEMA's efforts to measure preparedness has been limited due to, among other things, missing quantifiable metrics to measure capabilities. In April 2009, we reported that establishing quantifiable metrics for target capabilities was a prerequisite to developing assessment data that can be compared across all levels of government. At the time of our review, FEMA was in the process of refining the target capabilities to make them more measurable and planned to develop quantifiable metrics for each of the capabilities. We reported in October 2010 that FEMA had not yet developed national preparedness capability requirements based on established metrics to provide a framework for assessing preparedness. FEMA officials told us that evaluation efforts that they used to collect data on national preparedness capabilities were useful for their respective purposes, but that the data collected were limited by data reliability and measurement issues related to the lack of standardization. Until a framework for assessing preparedness is in place, we reported that FEMA would not have a basis on which to operationalize and implement its conceptual approach for assessing local, state, and federal preparedness capabilities against capability requirements and identify capability gaps for prioritizing investments in national preparedness. In our April 2009 report, we recommended that FEMA improve national preparedness by enhancing its project management plan for assessing capabilities to include reporting on the progress of preparedness assessments and developing quantifiable metrics for capabilities. DHS concurred, and in July 2011 FEMA reported that it took steps to establish a preparedness baseline and the accompanying foundation for assessing preparedness, including determining how effective grants are in improving preparedness. FEMA also reported that it was working with its emergency response partners to identify end-states, capabilities, and performance objectives for each emergency preparedness mission area as part of its development of the National Preparedness Goal. FEMA further will provide a summary of the progress being made towards developing and maintaining performance objectives required to deliver the capabilities described in the goal. In August 2011, FEMA reported that it had established a Program Executive Office to ensure that the target dates for implementation of Presidential Policy Directive 8 are met and stakeholders are engaged in the process. As these efforts are recent, we have not conducted work to assess their effectiveness in measuring preparedness. However, in the past FEMA has had difficulty meeting target dates, thus it will be important for FEMA to effectively consult with and incorporate the input of its many stakeholders to support meeting this schedule.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00856 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.482

Area	Overall assessment	Summary of key progress and work remaining
		DHS and FEMA have strengthened nationwide recovery planning efforts, but efforts are in the early stages. **Key progress:** In February 2010, FEMA released a draft National Disaster Recovery Framework, which is intended to provide a model to collectively identify and address challenges that arise during the disaster recovery process. This Framework is designed to help the emergency management community work better together to support individuals, households, and communities as they rebuild and restore their ways of life following a disaster. FEMA later reported that since March 2010, it has received hundreds of comments and recommendations from federal agencies and departments on the proposed Framework. In March 2010, we reported that FEMA assisted local communities with developing long-term disaster recovery plans as part of its post-disaster assistance. For example, one way FEMA assisted Iowa City's recovery from major floods in 2008 by, among other things, identifying possible federal funding sources for specific projects in the city's recovery plan and advising the city on how to prepare effective project proposals. Local officials credited this assistance with helping the city to be able to secure federal funding. **What remains to be done:** We have identified areas where FEMA's recovery assistance to local communities should be improved. For example, state and local officials in Texas recovering from Hurricane Ike in 2008 said that FEMA's process of ranking projects in the City of Galveston's recovery plan had the effect of fostering unrealistic expectations among the public about what projects would be funded. We recommended that FEMA more clearly communicate the objectives and processes it uses when assessing the value of specific recovery projects to help prevent unrealistic expectations about the implementation of such projects among members of the affected community. DHS agreed and stated that it would further examine the tools it used to communicate with impacted communities as part of the implementation of the National Disaster Recovery Framework. With regard to Framework, in July 2011, FEMA reported that the revised draft of the Framework was in the final stages of interagency review and interagency teams had been working to develop draft annexes for the six core functional areas of the Framework. Since FEMA has not yet finalized this framework, it is too early to assess its results.
Provision of emergency assistance and services	FEMA improved emergency assistance services and oversight of disaster-related emergency assistance, but should further strengthen its management of emergency response and recovery assistance programs.	**FEMA improved the provision and oversight of emergency assistance and services, but work remains in its management and operation of emergency response and recovery assistance programs.** **Key progress:** FEMA has provided and coordinated the provision of assistance to state and local governments, non-profit organizations, and individuals after disasters—including helping communities develop long-term recovery plans. In June 2011, the DHS IG reported that it had identified 128 programs that provide disaster assistance and that DHS administers 69, or approximately 54 percent, of these programs. For example, FEMA operates the Public Assistance program, which provides grants to state, local, and tribal governments and certain non-profit organizations.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00857 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.483

Area	Overall assessment	Summary of key progress and work remaining
		FEMA also took steps to improve its disaster assistance program oversight. In December 2008, we identified challenges in the Public Assistance program related to project development, information sharing and tracking the status of projects, project approvals and appeals, and human capital. For example, disagreements between applicants and FEMA, as well as changes to project scope decisions, contributed to slowing down project development. We reported that DHS had addressed these challenges, including finalizing a public assistance catastrophic disaster recovery concept plan that recognized the need to more easily tailor projects to meet post-disaster conditions; developing new management information systems to better track and manage projects and increase the transparency of public assistance funding; and creating a credentialing program for employees. Further, in July 2011, FEMA reported that it had established two Public Assistance review panels within the Public Assistance appeals process for the purpose of expediting final eligibility decisions for disputed projects. With respect to employee credentialing, FEMA reported in July 2011 that its newly created FEMA Qualification System is intended to build upon previous efforts to credential FEMA's disaster response personnel. According to FEMA, the system is expected to improve workforce qualification and certification of FEMA personnel deployed for incident management and support operations. We are conducting ongoing work related to FEMA's disaster assistance workforce and plan to report on our results in 2012.[f] **What remains to be done:** In March 2010, we identified two broad challenges related to FEMA's long-term disaster recovery assistance efforts. First, the criteria for when FEMA was to provide long-term recovery assistance in a specific disaster were vague, which resulted in uncertainty among other federal agencies and state recovery officials. Second, in some cases, FEMA assistance began before state and local governments had the capacity to effectively work with FEMA and ended before critical long-term recovery coordination and planning needs were fully addressed. We recommended, among other things, that DHS develop clear and consistent criteria that identify factors that determine whether and how the entity responsible for coordinating long-term recovery will become involved in a specific disaster. We also recommended that DHS establish a long-term recovery structure that more effectively aligns the timing and level of involvement of the entity responsible for coordinating long-term community recovery assistance with both the capacity of state and local governments to work with them and the need for coordination assistance. DHS concurred and reported in July 2011 that it had developed an assessment tool to assist a coordinating officer or state when attempting to determine if activating the long term recovery mission is appropriate. These are positive steps that should help strengthen FEMA's efforts to address timing issues with its disaster recovery, but they are still in the early stages of implementation.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00858 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.484

Area	Overall assessment	Summary of key progress and work remaining
		Additionally, FEMA reported in July 2011 that it sought to increase its disaster reservist cadre with professionals in areas of community planning, city management, and economic recovery to also provide an enhanced technical resource to local governments early in recovery efforts to assist in launching recovery planning. These are positive steps that should assist FEMA in its recovery efforts. However, because of the long-term nature of disaster recovery, it will take time to determine the impact of these efforts in enhancing recovery from such recent disasters as the tornados that devastated areas of Alabama and Missouri.
Emergency and interoperable communications	DHS and FEMA made strategic progress in enhancing emergency and interoperable communications. However, specific alert systems, such as the Integrated Public Alert and Warning System, have technical challenges, such as message delivery limitations.	**DHS and FEMA released key emergency communications strategic documents and made grants available for interoperability, but have made limited progress to enhance emergency alert systems.** **Key progress:** Continuity of communications, capacity, and interoperability are primary areas of vulnerability in emergency communications. Emergency communications breakdowns undermined response efforts during terrorist attacks in 2001 and Hurricane Katrina in 2005. In response, federal agencies, including DHS, increased efforts to enhance emergency communications. In June 2009, we reported that DHS and other federal agencies took steps to enhance emergency communications by issuing key documents such as the *National Emergency Communications Plan*—the first strategic document for improving emergency communications nationwide. Further, DHS and other federal agencies made numerous grants for interoperable communications available and increasingly aligned them with national and state plans. In addition, we reported that federal agencies, including DHS, took strategic steps to assist first responders. In March 2010, we reported that the Emergency Communications Preparedness Center had been established. At that time, the members were developing a working definition of the scope of emergency communications to define the scope of their mission and the types of information that should be included in an emergency communications clearinghouse. As of July 2011, DHS reported that the membership of the Preparedness Center expanded to 14 federal agencies, and the members had developed strategic objectives and an action plan to implement these objectives. FEMA also reported that it established and implemented working groups and a Disaster Emergency Communications Division to support emergency and interoperable communications.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00859 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.485

Area	Overall assessment	Summary of key progress and work remaining
		Further, in September 2009, we reported on the Emergency Alert System, the primary national-level public warning system, and FEMA's Integrated Public Alert and Warning System, which is intended to integrate new and existing alert capabilities, including the Emergency Alert System, into a "system of systems" to become the country's comprehensive public alert system. We reported that FEMA faced coordination issues in developing and implementing the system. For example, many stakeholders we contacted during our work knew little about the Integrated Public Alert and Warning System and expressed the need for better coordination with FEMA. Among other things, we recommended that FEMA develop strategic goals and processes for deployment of the Integrated Public Alert and Warning System and report periodically on program progress to the Congress and to the Secretary of Homeland Security in order to improve program transparency and accountability. DHS concurred and published an Integrated Public Alert and Warning System Strategic Plan in June 2010 that identified the vision, mission, goals and objectives of the program.[9] **What remains to be done:** In September 2009, we reported that FEMA faced technical challenges in implementing the Integrated Public Alert and Warning System related to systems integration, standards development, the development of geo-targeted and multilingual alerts, and alerts for individuals with disabilities. For example, FEMA's standard intended to facilitate integration of alert systems was under development and not widely used. As a result, we reported that integration with state and local systems would likely be a significant challenge due to potential incompatibility, and FEMA did not yet have logistical plans to integrate these systems. Further, we reported that to demonstrate the integration and expansion of new alerting technologies, and to work toward the functionality described in the executive order, FEMA had implemented pilot projects, but they ended inconclusively, with few documented lessons learned. We recommended, among other things, that FEMA establish and implement a plan to verify the dependability and effectiveness of systems used to disseminate alerts. FEMA concurred and, in July 2011, reported that it had engaged with a range of agencies, organizations, and private sector entities to promote Integrated Public Alert and Warning System capabilities and opportunities for the integration of alert and warning technologies for people with access and functional needs. FEMA reported that it had partnered with organizations to demonstrate products that incorporate technologies for alerting persons with access and functional needs. Further, FEMA reported that it was developing an infrastructure of alert and warning capabilities that expands on the traditional Emergency Alert System by, for example, allowing individuals with enabled mobile devices to receive text-like messages alerting them of imminent threats in their geographic area. FEMA reported that in March 2011 it deployed the Integrated Public Alert and Warning System-Open Platform for Emergency Networks, a set of securely hosted Web services that enable the routing of alerts and warnings between various third-party systems, networks, and devices. As DHS has recently implemented this system and its pilot products have not yet been deployed, it is too early to assess the effectiveness of these efforts.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00860 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.486

Area	Overall assessment	Summary of key progress and work remaining
Support to state and local partners	FEMA made progress in allocating homeland security grants using a reasonable risk assessment methodology. However, challenges remain regarding the coordination of grant programs.	**FEMA used a reasonable risk assessment methodology to allocate the Urban Areas Security Initiative and State Homeland Security grants, but FEMA should coordinate the application and review process for its preparedness grants.** **Key progress:** Within FEMA, the Grant Programs Directorate is responsible for business operations, training, policy, oversight of all FEMA grants, and the program management of preparedness grants. FEMA's grant programs vary from enhancing capabilities that focus on counterterrorism and catastrophic events, to specific first-responder disciplines that strengthen capabilities for addressing hazards of all types. For example, the State Homeland Security Program provides funding in an effort to address the identified planning, organization, equipment, training, and exercise needs at the state and local levels to prevent, protect against, respond to, and recover from acts of terrorism and other catastrophic events. The Urban Areas Security Initiative program provides funding to address the unique planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism. In June 2008, we reported that DHS had constructed a reasonable methodology to assess risk and allocate the Urban Area Security Initiative and State Homeland Security grants, but that this methodology did not account for vulnerability differences among jurisdictions. In July 2011, DHS reported that it modified its methodology for fiscal year 2011 to address the measurement of vulnerability in its risk-based grant allocation model. Specifically, FEMA reported creating a separate vulnerability assessment that accounts for 20 percent of the overall risk assessment for states, and territories, and the top 100 metropolitan areas for use in the State Homeland Grant Program and the Urban Areas Security Initiative grant program. We have ongoing work assessing these homeland security grant programs, and plan to report on the results later this year.[h] **What remains to be done:** In March 2011 we reported that until FEMA evaluates grant applications across grant programs, FEMA cannot ascertain whether or to what extent multiple funding requests are being submitted for similar purposes. In March 2010, the DHS IG reported that FEMA should improve the efficacy of the grant application and review process by taking steps to mitigate duplication or redundancy within the agency's various preparedness grant programs. Specifically, the DHS IG found that FEMA's grant application process risked being ineffective because it did not compare and coordinate grant applications across programs to identify and mitigate potential duplications. Additionally, grant application processes were not efficient, requiring FEMA and state and local grant administrators to expend time and resources fulfilling redundant requirements for the numerous grant programs.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00861 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.487

Area	Overall assessment	Summary of key progress and work remaining
		The IG recommended, among other things, that FEMA identify grant programs that may overlap or duplicate with other programs. FEMA concurred and reported it planned to take action to address them. For example, FEMA reported in July 2011 that it was working with DHS and other federal departments to consolidate existing preparedness grant programs and entering into a memorandum of understanding with the Departments of Health and Human Services and Transportation to clarify roles among the departments regarding their emergency preparedness-related grants. These are positive steps and should help strengthen FEMA's grant management. However, our work and that of the DHS IG has shown that FEMA should further benefit from examining its grant programs and coordinating its application process to eliminate or reduce redundancy among grant recipients and program purposes.

Source: GAO analysis

Note: This table also includes examples from selected DHS IG reports.

[a] The Post-Katrina Emergency Management Reform Act required the Secretary of Homeland Security to establish a National Advisory Council to advise the FEMA Administrator on all aspects of emergency management. Among its specific responsibilities, the Council was to incorporate input from state, local, and tribal governments as well as the private sector in the development and revision of the 2004 *National Response Plan*. 6 U.S.C. § 318.

[b] In July 2011, FEMA reported that it had begun using a "Whole Community" approach in which it was engaging non-federal stakeholders in its preparedness planning efforts. For example, FEMA reported that, in implementing elements of Presidential Policy Directive 8, which was issued on March 30, 2011, it had engaged non-federal stakeholders, such as the National Advisory Council, the Local, State, Tribal and Federal Preparedness Task Force and state and local associations. FEMA also reported taking steps to increase private sector participation by, among other things, creating a private sector division to increase coordination during disaster planning, response and recovery efforts, such as National Level Exercise 2011, establishing a seat for a private sector representative to work with FEMA and other federal partners at the National Response Coordination Center, and planning to incorporate private sector and nongovernmental representatives to participate in response and recovery exercises.

[c] The National Incident Management System presents, among other things, doctrine that standardizes the process for emergency response stakeholders to conduct integrated emergency management and incident response operations by establishing organizational incident management structures.

[d] The *National Response Framework* Emergency Support Function Annexes align categories of federal government response resources and capabilities and provide strategic objectives for their use under the *National Response Framework*. The *National Response Framework* Support Annexes describe the roles and responsibilities of federal departments and agencies and nonfederal entities in coordinating and executing the common functional processes and administrative requirements necessary for incident management that are common to all incidents.

[e] The implementation plan for Presidential Policy Directive 8 includes target dates for the first edition of a national preparedness goal (September 25, 2011), a document describing the national preparedness system (November 24, 2011), the first national preparedness report (March 30, 2012), the first edition of the national planning frameworks (June 30, 2012) and the first edition of the interagency operational plans to support the delivery of capabilities in each of the frameworks (September 25, 2012).

[f] We are conducting this review at the request of the House Committee on Homeland Security and the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Senate Committee on Homeland Security and Governmental Affairs and plan to report on the results of our review in 2012.

[g] Federal Emergency Management Agency. *Strategic Plan for the Integrated Public Alert and Warning System (IPAWS) Program*. June 2010.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00862 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.488

[h] We are conducting this work for the House Committee on Homeland Security; the Senate Committee on Homeland Security and Governmental Affairs; and the Senate Committee on Commerce, Science, and Transportation.

GAO Contacts

For additional information about this area, contact William O. Jenkins, Jr. at (202) 512-8757 or jenkinswo@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00863 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.489

Appendix XIII: Department of Homeland Security Transformation and Implementation

What This Area Includes

In 2003, we designated implementing and transforming the Department of Homeland Security (DHS) as high risk because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to effectively address DHS's management and mission risks could have serious consequences for U.S. national and economic security. This high-risk area includes challenges in strengthening DHS's management functions, the impact of those challenges on DHS's mission implementation, and challenges in integrating management functions within and across the department and its components.[1]

For the purposes of this report, we are highlighting examples of DHS transformation and implementation efforts in key areas on which we have recently reported, and not on areas on which we have not reported or have conducted limited audit work. DHS has other transformation and implementation efforts underway at the department and component levels. We have not completed work on these areas upon which to base an assessment of DHS's progress.

Key Progress and Work Remaining

DHS has strengthened its management functions. For example, the department revised its acquisition management oversight policies to include more detailed guidance to inform departmental acquisition decision making. DHS also developed corrective action plans for financial management weaknesses, and the number of conditions contributing to departmentwide material weaknesses has declined at the component level since 2005.[2] Further, DHS issued its *Workforce Strategy for Fiscal Years 2011-2016* in December 2010, which contains the department's

[1] We define management integration as the development of consistent and consolidated processes, systems, and people—in areas such as information technology, financial management, procurement, and human capital—as well as in its security and administrative services, for greater efficiency and effectiveness.

[2] A material weakness is a significant deficiency, or a combination of significant deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00864 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.490

workforce goals, objectives, and performance measures for human capital management. However, DHS continues to face significant weaknesses in these areas that hinder the department's transformation efforts and its ability to meet its missions. For example, because of acquisition and information technology management weaknesses, major programs have not met capability, benefit, cost, and schedule expectations. Further, we reported that financial management internal control weaknesses have impeded DHS from providing reliable and timely financial data to support daily operational decision making. Moreover, human capital challenges have affected departmental and component efforts to implement their missions. As DHS continues to mature as an organization, it will be critical that the department continue to work to strengthen its management functions and their implementation, since the effectiveness of these functions and their implementation directly affects its ability to fulfill its homeland security and other missions.

DHS has developed and begun to implement its strategy to address the high-risk area, but has not yet demonstrated sustainable, measurable progress in its implementation efforts. In our 2011 high-risk update, we reported that DHS has taken action to implement, transform, and strengthen its management functions. The Secretary and Deputy Secretary of Homeland Security, and other senior officials, have demonstrated commitment and top leadership support to address the department's management challenges. In January 2011, DHS provided us with its *Integrated Strategy for High Risk Management*, which summarized the department's preliminary plans for addressing the high-risk area, and DHS updated this strategy in June 2011. We provided DHS with feedback on the January 2011 strategy and have worked with the department to monitor implementation efforts. For example, we noted that the January 2011 strategy was generally responsive to actions and outcomes we identified for the department to address the high-risk area. However, we noted that, in most cases, the strategy did not identify the specific resources needed to implement planned corrective actions, making it difficult to assess the extent to which DHS has the capacity to implement these actions. Additionally, we noted that the strategy did not provide information on the underlying metrics or factors DHS used to rate its progress, making it difficult for us to assess DHS's overall characterizations of progress. In the June 2011 update, DHS provided ratings of its progress in implementing corrective actions related to each management function. We are assessing DHS's ratings and the June 2011 update, and plan to provide the department with our feedback later this year.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00865 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.491

Going forward, to address the long-standing problems in its management functions and in the integration of those functions, DHS needs to implement its *Integrated Strategy for High Risk Management*; continue its efforts to identify and acquire resources needed to achieve key actions and outcomes; implement a program to monitor and validate its corrective actions; and show measurable, sustainable progress in implementing corrective actions and achieving key outcomes.

DHS developed processes and policies for managing its acquisitions, but faces significant challenges in ensuring proper implementation. DHS has taken steps to strengthen acquisition oversight processes, but it continues to face obstacles in managing its acquisitions and ensuring proper implementation and departmentwide coordination. We previously reported that DHS faced challenges related to acquisition oversight, cost growth, and schedule delays. In August 2007, DHS established the Acquisition Program Management Division under the Office of the Chief Procurement Officer to help strengthen acquisition management within the department. Further, in June 2010, we reported that DHS continued to develop its acquisition oversight function and had begun to implement a revised acquisition management directive that includes more detailed guidance for programs to use when informing component and departmental decision making. We also reported that the senior-level Acquisition Review Board had met more frequently and provided programs decision memorandums with action items to improve performance.[3] However, while the Acquisition Review Board reviewed 24 major acquisition programs in fiscal years 2008 and 2009, more than 40 major acquisition programs had not been reviewed, and programs had not consistently implemented action items identified as part of the review by established deadlines. In July 2011, DHS reported that the Acquisition Program Management Division in 2009 started conducting annual portfolio program reviews with components with the goal of ensuring that major programs receive at least one review on an annual basis, and that DHS had conducted reviews of additional programs through the Acquisition Review Board in fiscal years 2010 and 2011.

[3] The Acquisition Review Board is the DHS executive board that reviews major acquisition programs. Among other things, the board reviews select acquisitions for executable business strategy, resources, management, accountability, and alignment to strategic initiatives. It also approves acquisitions to proceed to their next acquisition life-cycle phases upon satisfaction of applicable criteria.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00866 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.492

Our work has also shown that departmental concerns exist about the accuracy of cost estimates for some of DHS's major programs.[4] In addition, over half of the programs we reviewed for our June 2010 report awarded contracts to initiate acquisition activities without component or department approval of documents essential to planning acquisitions, such as mission need statements outlining the specific functional capabilities required to accomplish DHS's mission and objectives; operational requirements; and acquisition program baselines. Additionally, in November 2010, leveraging our work, the DHS Office of Inspector General (IG) identified acquisition management as a major challenge facing the department. We have made a number of recommendations to DHS to strengthen its acquisition management functions, such as establishing a departmental joint requirements oversight board to review and approve acquisition requirements, and ensuring major investments comply with established component and departmental review policy standards. DHS generally agreed and is working to address them by, among other things, establishing an Investment Review Board to help oversee the status of all acquisition investments; expanding its Acquisition Corps to provide trained procurement and program management professionals to manage DHS's most critical acquisition programs; developing a tool to track programs' cost, schedule, and performance indicators; and evaluating the effectiveness of award fees and performance incentives. These are positive actions that should better position DHS to meet its acquisition needs. However, moving forward, DHS will need to continue to demonstrate sustainable progress in implementing these actions and delivering programs that meet cost, schedule, and performance expectations.

DHS established information technology management controls, capabilities, and policies, but gaps remain in implementing management policies and procedures. DHS established information technology management controls and capabilities, but in September 2009 we reported that DHS made uneven progress in its information technology management efforts to institutionalize a framework of

[4] In June 2008, DHS established the Cost Analysis Division to help validate cost estimates. In July 2011, DHS reported that it plans to combine this division with the Acquisition Program Management Division to create a new office—tentatively called the Office of Program Accountability and Risk Management—to report directly to the Under Secretary for Management.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00867 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.493

interrelated management controls and capabilities. For example, DHS continued to issue annual updates to its enterprise architecture that added previously missing scope and depth, and further improvements were planned to incorporate the level of content, referred to as segment architectures, needed to effectively introduce new systems and modify existing ones.[5] In addition, in July 2011, DHS reported that the department had begun tracking implementation of our Enterprise Architecture Management Maturity Framework and had developed plans to improve enterprise architecture maturity within each component and departmentwide.[6] We further reported that DHS redefined its information technology acquisition and investment management policies, practices, and structures, including establishing a system life cycle management methodology, and increased its information technology acquisition workforce.[7] In addition, in August 2011, DHS reported that it had efforts underway to establish an information technology program manager certification track intended to assist in managing information technology program management challenges.

Nevertheless, challenges remain relative to, for example, fully defining key system investment and acquisition management policies and procedures for information technology. Moreover, the extent to which DHS implemented these investment and acquisition management policies and practices on major information technology programs has been inconsistent. For example, our work showed that major information technology acquisition programs were not subjected to executive-level acquisition and investment management reviews. As a result, major programs aimed at delivering important mission capabilities had not lived up to their capability, benefit, cost, and schedule expectations.

We also reported on challenges departments, including DHS, have faced in implementing controls to protect their computer systems and networks. For example, we reported on the need for federal agencies, including DHS, to improve implementation of information security controls, such as

[5] Enterprise architecture is a corporate blueprint that serves as an authoritative frame of reference for information technology investment decision making.

[6] Our Enterprise Architecture Management Maturity Framework provides a practical approach for incrementally developing and implementing an enterprise architecture.

[7] A system life cycle management process normally begins with initial concept development and continues through requirements definition to design, development, various phases of testing, implementation, and maintenance.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00868 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.494

those for configuring desktop computers and wireless communication devices. Additionally, in November 2010, the DHS IG identified information technology management as a major challenge facing the department. For example, the DHS IG reported that the department faces challenges as it attempts to create a unified information technology infrastructure for effective integration and agencywide management of information technology assets and programs. We made recommendations to strengthen DHS information technology management, such as establishing procedures for implementing project-specific investment management policies, and policies and procedures for portfolio-based investment management. DHS is working to strengthen these areas by, for example, developing a process for information technology acquisition management to help ensure that each investment begins with a successful plan and road map for its life cycle and by establishing executive steering committees to monitor the cost and schedule performance of all high-risk information technology investments. While these are positive steps that should better position the department in managing its information technology investments moving forward, DHS will need to continue to make measurable progress in implementing these actions and successfully developing and deploying information technology programs.

DHS took steps to address financial management weaknesses, but faces challenges in modernizing its financial systems and has been unable to obtain an unqualified audit opinion. DHS made progress in addressing its financial management and internal controls weaknesses. For example, DHS reduced the number of conditions at the component level contributing to departmentwide material weaknesses since 2005. However, DHS twice attempted to implement an integrated departmentwide financial management system, but has not been able to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00869 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.495

consolidate its disparate systems.[8] In addition, DHS has not been able to obtain an unqualified audit opinion on its consolidated financial statements (i.e., prepare a set of financial statements that are considered reliable). For fiscal year 2010, the independent auditor issued a disclaimer on DHS's consolidated financial statements and identified deficiencies in DHS's internal control over financial reporting. Until these weaknesses are resolved, DHS will not be in position to provide reliable, timely, and useful financial data to support day-to-day decision making. In addition, as a result of these weaknesses, in November 2010 the DHS IG assessed financial management as one of the major management challenges facing the department. DHS has taken steps to prepare and implement corrective action plans for its internal control weaknesses through its *Internal Control Playbook*, DHS's annual plan to design and implement departmentwide internal controls. Further, in fiscal year 2010 DHS committed to the goal of receiving a qualified audit opinion on its consolidated balance sheet in fiscal year 2011, and the department is working toward that goal by, for example, focusing on strengthening budgetary resource processes and payment management, and remediating financial management issues at the U.S. Coast Guard. These are positive first steps toward achieving a successful full scope audit of the department's consolidated financial statements and, if implemented effectively, should help DHS strengthen its financial management functions.

DHS issued plans for human capital activities, but has not yet fully addressed barriers to equal opportunity employment and assessed foreign language workforce needs and gaps. DHS issued various strategies and plans for its human capital activities and functions. For example, in December 2010 DHS issued its *Workforce Strategy for Fiscal Years 2011-2016,* which contains the department's workforce goals,

[8] Since its creation, DHS has made two attempts to implement an integrated departmentwide financial management system—first through its Electronic Managing Enterprise Resources for Government Efficiency and Effectiveness program and second through its Transformation and Systems Consolidation program. As we reported in June 2007, DHS had ended its Electronic Managing Enterprise Resources for Government Effectiveness and Efficiency effort after determining that the resulting financial management systems would not provide the expected system functionality and performance. In December 2009, we reported that the Transformation and Systems Consolidation program had been affected by bid protests and related litigation which was contributing to a significant delay in awarding a contract. DHS ended this program in May 2011 and reported that moving forward it would consider alternatives to meet revised requirements.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00870 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.496

objectives, and performance measures for human capital management. These strategies are promising, but DHS has faced challenges in implementing its human capital functions, including hiring people with the needed skills and abilities in areas such as acquisition management, for example. Further, our prior work suggests that successful organizations empower and involve their employees to gain insights about operations from a frontline perspective, increase their understanding and acceptance of organizational goals and objectives, and improve motivation and morale. However, DHS's scores on the Partnership for Public Service's 2010 rankings of the Best Places to Work in the Federal Government improved from prior years, but in 2010, it was ranked 28 out of 32 agencies in the Best Places to Work ranking on overall scores for employee satisfaction and commitment.[9]

In addition, our prior work identified several workforce barriers to achieving equal employment opportunities and the identification of foreign language needs and capabilities at DHS. In August 2009 we reported that DHS developed a diversity council, among other initiatives, but that DHS generally relied on workforce data and had not regularly included employee input from available sources to identify triggers to barriers to equal employment opportunities, such as promotion and separation rates. In June 2010 we reported on DHS's foreign language capabilities, noting that DHS took limited actions to assess its foreign language needs and existing capabilities and to identify potential shortfalls.[10] Assessing hiring needs is crucial in achieving a range of component and departmentwide missions. We recommended that DHS incorporate employee input in identifying potential barriers to equal employment opportunities and comprehensively assess its foreign language needs and capabilities. DHS concurred and reported having actions underway to address the recommendations, such as launching an exit survey across DHS in fiscal year 2011 to help use employee input to identify equal employment opportunity barriers, developing a task force to identify foreign language requirements, completing two foreign language assessments departmentwide, and planning to establish a language services executive

[9] Partnership for Public Service and the Institute for the Study of Public Policy Implementation at the American University School of Public Affairs, *The Best Places to Work in the Federal Government* (Washington, D.C.: 2010).

[10] DHS has a variety of responsibilities that utilize foreign language capabilities, including investigating transnational criminal activity and staffing ports of entry into the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00871 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.497

steering committee to provide oversight of the department's language requirements. DHS reported that it is also working to address its human capital management challenges by, among other things, developing component operational plans for the *Workforce Strategy,* tracking those plans against a common set of performance measures, and implementing comprehensive workforce planning to link the department's strategic goals, mission critical occupations, and workforce capacity and capabilities. These are positive actions that should better position DHS in assessing and meeting its human capital needs, but more work remains.

DHS took action to integrate its management functions, but needs to continue to demonstrate sustainable progress in integrating those functions within and across the department and its components. DHS took action to integrate its management functions. For example, DHS put in place common policies, procedures, and systems within individual management functions, such as human capital, that help to integrate its component agencies. In November 2009, we reported that DHS had not yet developed a strategy for management integration with characteristics we recommended, such as clearly identifying critical links that must occur among management initiatives and identifying potential efficiencies. In the January 2011 *Integrated Strategy for High Risk Management,* as well as the June 2011 update, DHS included a management integration plan containing information on ongoing and planned initiatives to integrate its management functions within and across the department and its components. For example, DHS plans to establish a framework for managing investments across its components and management functions to strengthen integration within and across those functions, as well as to ensure mission needs drive investment decisions. This framework seeks to enhance DHS resource decision making and oversight by creating new department-level councils to identify priorities and capability gaps, revising how DHS components and lines of business manage acquisition programs, and developing a common framework for monitoring and assessing implementation of investment decisions. These actions, if implemented effectively, should help to further and more effectively integrate the department. We also reported that DHS needs to continue to implement corrective actions within individual management areas, such as acquisition and financial management, to develop consistent or consolidated processes and systems within and across the department and its components. DHS is working to implement these corrective actions which, if implemented effectively, should help DHS drive integration of its management functions. Going forward, we will continue to review and provide feedback

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00872 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.498

on DHS's updated plan for management integration and will monitor implementation efforts.

GAO Contacts

For additional information about this area, contact David Maurer at (202) 512-9627 or maurerd@gao.gov for transformation, human capital management, and management integration; John Hutton at (202) 512-4841 or huttonj@gao.gov for acquisition management; David A. Powner at (202) 512-9286 or pownerd@gao.gov for information technology management; or Paula Rascona at (202) 512-9816 or rasconap@gao.gov for financial management.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00873 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.499

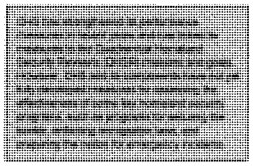
Appendix XIV: Performance Measurement

What This Area Includes

Performance measurement underpins federal efforts to assess and report on progress in strengthening programs and operations. We reported on the importance of the development of outcome-based performance goals and measures as part of results management efforts across government. Performance goals and measures are intended to provide Congress and agency management with information to systematically assess a program's strengths, weaknesses, and performance. A performance goal is the target level of performance expressed as a tangible, measurable objective against which actual achievement will be compared. A performance measure can be defined as an indicator, statistic, or metric used to gauge program performance. Outcome-oriented measures show results or outcomes related to an initiative or program in terms of its effectiveness, efficiency, or impact.

For the purposes of this report, we are generally highlighting examples of Department of Homeland Security (DHS) performance measurement efforts in key areas on which we have recently reported, and not on areas on which we have not reported or have conducted limited audit work. DHS has other performance measurement efforts underway at the department and component levels. We have not completed work on these areas upon which to base an assessment of DHS's progress.

Key Progress and Work Remaining



DHS has strengthened its performance measures, but has not yet fully developed outcome-based measures for assessing progress and performance for many of its mission functions. Over the past 3 years, DHS has strengthened its performance measures. In 2007, we reported on progress made by DHS in implementing its mission and management functions by assessing actions taken by DHS to achieve performance expectations set for the department in legislation, presidential directives, and DHS and component strategic plans and documents.[1] We noted that DHS generally had not established quantitative goals and measures for assessing its performance and, as a result, we could not assess where along a spectrum of progress DHS stood in achieving these expectations. At the request of the Senate Committee on Homeland Security and Governmental Affairs following the issuance of that report, we provided DHS with feedback on the

[1] The performance expectations we identified for DHS in this report do not represent performance goals or measures for the department.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00874 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.500

department's performance goals and measures to help strengthen DHS's efforts in this area. Our feedback was based on our work on and subject matter knowledge of the programs, activities, and areas being measured, as well as our work on effective practices for performance measurement. This feedback ranged from pointing out components' limited use of outcome-oriented performance measures to assess the results or effectiveness of programs, to raising questions about the steps DHS or its components took to ensure the reliability and verification of performance data. DHS also implemented internal efforts to strengthen its performance measures. For example, as part of our ongoing review of the QHSR, we found that DHS worked to align its performance measures to the QHSR missions and goals.[2] The department also provided components with guidance that outlines how to assess QHSR missions and related training, and formed working groups to discuss implementing specific performance measure concepts. Further, DHS reported that after the QHSR was issued, DHS senior leaders held meetings to discuss how to revise existing performance measures, and components worked to develop improved performance measures.

In response to its internal efforts and our feedback, DHS developed and revised its performance goals and measures for some areas to strengthen its ability to assess its outcomes and progress. For fiscal year 2011, DHS identified 85 strategic measures for assessing its progress in achieving its QHSR missions and goals. In addition to these strategic measures, the department has 132 management measures, which DHS uses for assessing programmatic performance and for resource allocation and other internal decision making purposes, such as program evaluation. In addition, in July 2011, DHS reported that the department has identified 24 areas for focused efforts to develop enhanced measures, based on guidance from DHS leadership and the Office of Management and Budget. These areas address gaps in both strategic and management measures for specific mission areas. DHS also plans to continue its annual process for reviewing and working to strengthen its performance measures.

While DHS has made progress in strengthening performance measurement, our work across the department has shown that a number

[2] We are conducting this review at the request of the Senate Committee on Homeland Security and Governmental Affairs and plan to report on our results later this year.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00875 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.501

of programs lack outcome goals and measures, which may hinder the department's ability to effectively assess results or fully assess whether the department is using resources effectively and efficiently. We have recognized that DHS faces some inherent difficulties in developing performance goals and measures to address its unique mission and programs, such as in developing measures for the effectiveness of its efforts to prevent and deter terrorist attacks. In such instances, proxy measures—or indirect indicators—should be designed to assess the effectiveness of program functions. Outcome measures are helpful to departmental decision makers and managers, as they describe the products and services delivered by a program over a period of time. However, we have reported that many of DHS's components have not developed adequate proxy or outcome-based performance measures or mechanisms to monitor, assess, and evaluate the effectiveness of their plans and performance. Such measures, along with output and process measures, would help DHS track progress being made toward specific goals and provide managers with important information upon which to base their decisions.

Our work has shown that DHS and its components did not have performance measures for assessing the effectiveness of key border security and immigration programs. For example, in September 2009 we reported that U.S. Customs and Border Protection (CBP) had invested $2.4 billion in tactical infrastructure (fencing, roads, and lighting) along the southwest border under the Secure Border Initiative—a multiyear, multibillion dollar program aimed at securing U.S. borders and reducing illegal immigration. However, DHS could not measure the impact of this investment in tactical infrastructure on border security. We recommended that DHS conduct an evaluation of the impact of tactical infrastructure on effective control of the border. DHS concurred and reported considering using independent researchers for evaluations. We also reported in August 2009 that CBP had established three performance measures to report the results of checkpoint operations, which provided some insight into checkpoint activity.[3] However, the measures did not indicate if checkpoints were operating efficiently and effectively and data reporting and collection challenges hindered the use of results to inform Congress and the public on checkpoint performance. We recommended that CBP

[3] CBP operates checkpoints on U.S. roads, mainly in Southwest border states, at which agents screen vehicles for unauthorized aliens and contraband.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00876 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.502

improve the measurement and reporting of checkpoint effectiveness. CBP agreed and reported plans to develop and better use data on checkpoint effectiveness.

Further, we reported that U.S. Immigration and Customs Enforcement (ICE) and CBP did not have measures for assessing the performance of key immigration enforcement programs. For example, in April 2011 we reported that ICE did not have measures for its overstay enforcement efforts, and in July 2010 that CBP did not have measures for its alien smuggling investigative efforts, making it difficult for these agencies to determine progress made in these areas and evaluate possible improvements. We recommended that ICE and CBP develop performance measures for these two areas. They generally agreed and reported actions underway to develop these measures. In addition, in July 2011, DHS stated that CBP was leading a multiyear effort to develop measures for border security to position the department to be able to assess the impact of security measures, such as tactical infrastructure, on border security. DHS also reported that it has measures for assessing its border security and immigration enforcement efforts, such as measures related to detaining and removing criminal aliens while maintaining compliance with detention standards. However, our work has shown that within key border security and immigration enforcement programs, DHS and its components can strengthen its measures for assessing program results.

In addition, with regard to emergency preparedness and response, we reported that DHS lacks measures for assessing the effectiveness of its preparedness and response efforts. For example, in March 2011 we reported that it has been difficult for the Federal Emergency Management Agency (FEMA) to overcome challenges in its efforts to measure preparedness and establish a system of metrics to assess national preparedness capabilities. In October 2010, we reported that FEMA officials said that evaluation efforts they used to collect data on national preparedness capabilities were useful for their respective purposes, but that the data collected were limited by data reliability and measurement issues related to the lack of standardization in the collection of data. Further, in January 2010 we reported that FEMA faced challenges measuring performance for its Citizen Corps Programs, its partner programs, and the Ready Campaign—community preparedness programs—because it relied on states to verify data for local program

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00877 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.503

units and was unable to control the distribution of the Ready Campaign messages or measure whether the messages were changing the behavior of individuals.[4] We noted that by examining the feasibility of approaches to verify data on its community preparedness programs, FEMA would be better positioned to begin to explore why programs that no longer exist were disbanded and develop possible strategies for reconstituting local programs or developing new ones. Among other things, we recommended that FEMA examine the feasibility of developing various approaches for ensuring the accuracy of program data.

In July 2011, FEMA reported taking additional action to strengthen its performance measures by, for example, implementing a priority goal focusing on ensuring resilience to disasters by strengthening disaster preparedness and response capabilities, and beginning in fiscal year 2010, requiring its offices to develop and report on activity-level (or operational level) performance measures to align to each of FEMA's budget activity lines. These steps should help FEMA strengthen its performance measurement efforts. However, FEMA should continue to work toward implementing a comprehensive set of measures for assessing national preparedness capabilities.

GAO Contact

For additional information about this area, contact David Maurer at (202) 512-9627 or maurerd@gao.gov.

[4] Citizen Corps is coordinated nationally by FEMA and is intended to help coordinate volunteer activities for, among other things, better preparing communities to respond to emergency situations. Citizen Corps programs build on the successful efforts that are in place in many communities around the country to prevent crime and respond to emergencies. Programs that started through local innovation are the foundation for Citizen Corps and this national approach to citizen participation in community safety.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00878 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.504

Appendix XV: Risk Management

What This Area Includes

Risk management has been widely supported by the President and Congress as a management approach for homeland security.[1] According to the Department of Homeland Security (DHS), risk information is usually one of many factors—and typically not the sole factor—that departmental decision makers consider when deciding which strategy to pursue. We have previously reported that defining an acceptable, achievable (within constrained budgets) level of risk is imperative to address current and future threats, and on the need to make risk-informed decisions related to homeland security. Many have pointed out, as did the Gilmore and 9/11 Commissions, that the nation will never be completely safe and total security is an unachievable goal.[2] Within its sphere of responsibility, DHS cannot afford to protect everything against all possible threats. As a result, DHS must make choices about how to allocate its scarce resources to most effectively manage risk, and a risk management approach can help inform these decisions.

To provide guidance to agency decision makers, we developed a risk management framework which is intended to be a starting point for applying risk-informed principles. Our risk management framework, shown in figure 2, entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

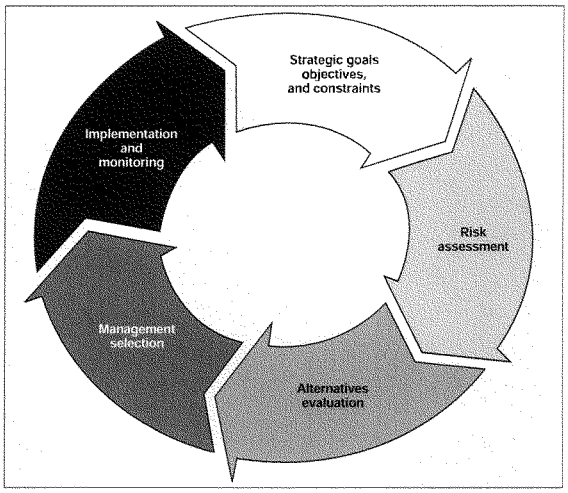
[1] The *DHS Risk Lexicon* defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. DHS further defines risk as the potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence. A threat is defined as natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability is defined as the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Consequence is defined as the effect of an event, incident, or occurrence. DHS, *DHS Risk Lexicon: 2010 Edition* (Washington, D.C.: September 2010).

[2] The Gilmore Commission's full name was the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. The 9/11 Commission was a bipartisan commission chartered to review the circumstances surrounding the September 11, 2001, terrorist attacks, including preparedness for and the immediate response to the attacks, and to provide recommendations designed to guard against future attacks.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00879 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.505

Figure 2: GAO Risk Management Framework



Source: GAO.

The *National Infrastructure Protection Plan*, issued by DHS, includes a risk analysis and management framework for the critical infrastructure community, which generally mirrors our framework. Like our framework, the *National Infrastructure Protection Plan's* risk management framework is a process that continuously uses the results of each step to inform the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00880 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.506

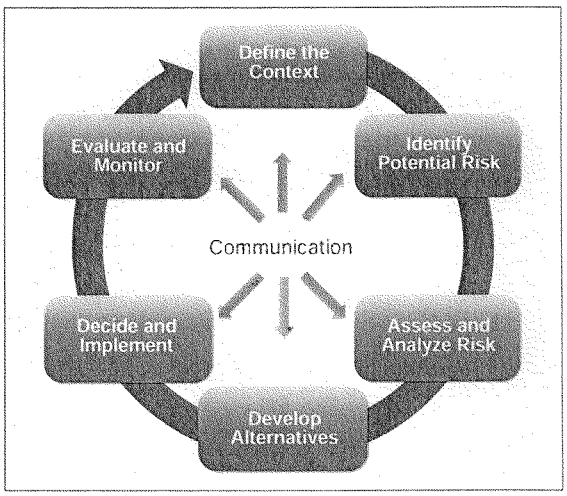
activities in both subsequent and previous steps over time.[3] The *National Infrastructure Protection Plan* risk management framework is designed to produce a systematic and comprehensive understanding of risk and ultimately provide for security investments based on this knowledge of risk. In addition, according to DHS, the Secretary's policy for integrated risk management and the department's *Risk Management Fundamentals: Homeland Security Risk Management Doctrine,* identify a risk management process to support decision making at DHS, as shown in figure 3.

[3] In accordance with the Homeland Security Act and in response to Homeland Security Presidential Directive 7, DHS issued, in June 2006, the first *National Infrastructure Protection Plan,* which provides the overarching approach for integrating the nation's critical infrastructure protection initiatives in a single effort. The plan sets forth a risk management framework and details the roles and responsibilities of DHS and other federal, state, regional, local, tribal, territorial, and private sector partners, including how they should use risk management principles to prioritize protection activities within and across sectors.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00881 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.507

Figure 3: DHS Risk Management Framework



Source: DHS.

For the purposes of this report, we are generally highlighting examples of key DHS areas related to risk management on which we recently reported, and not areas on which we have not reported or have conducted limited audit work. While this section focuses on key areas on which we have reported, such as risk assessments for transportation modes, DHS has implemented additional efforts related to risk management, such as various risk assessment tools, databases, and coordination mechanisms. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

DHS and its component agencies developed strategies and tools for risk management and conducted risk assessments. However, they should strengthen their use of risk information to inform their

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00882 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.508

[redacted]

planning and investment decision-making. DHS took action to develop various strategies, plans, and tools for risk management. For example:

- In 2007 DHS established the Risk Steering Committee, comprised of representatives from DHS's offices and components, to serve as the department's risk management governance body, setting policy and developing guidance for integrating risk management approaches.
- In January 2009 DHS published its *Integrated Risk Management Framework*, which, among other things, calls for DHS to use risk assessments to inform decision-making. Further, in October 2009, under the auspices of the 2010 Quadrennial Homeland Security Review (QHSR), DHS developed the Homeland Security National Risk Assessment methodology for assessing risk across a range of hazards for use by DHS in its decisions on strategy and policy development, planning priorities, resource allocation, and capability requirements development. As part of our ongoing review of DHS's 2010 QHSR, we found that DHS has not yet conducted a national risk assessment, but plans to conduct such an assessment as part of the next QHSR, which DHS plans to initiate in fiscal year 2012.[4]
- In May 2010, the Secretary issued a Policy Statement on Integrated Risk Management, calling for DHS and its partners to manage risks to the nation. DHS reported that it is developing doctrine and guidance to enable DHS to achieve integrated risk management and that DHS's *Integrated Risk Management Framework*, over time, will provide governance, policies, processes, tools, training, and accountability mechanisms for integrated risk management.
- DHS developed the Risk Assessment Process for Informed Decision-making tool to support DHS risk management tradeoffs. According to DHS, this tool has three key deliverables: (1) a quantitative multi-hazard homeland security risk baseline (i.e. annualized expected loss across a range of terrorism, transnational crime, and natural hazard events), (2) a map of major DHS programs to homeland security hazards that shows how programs interact to manage the risk of a specific hazard, and (3) program-based risk reduction analysis that shows the risk reduction of individual programs.
- In June 2010 the Transportation Security Administration (TSA) produced the *Transportation Sector Security Risk Assessment*, which incorporated threat, vulnerability, and consequence to assess risk

[4] We are conducting this work at the request of the Senate Committee on Homeland Security and Governmental Affairs and plan to report on the results later this year.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00883 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.509

within and across the various aviation and surface transportation modes, such as freight rail, passenger rail, and pipelines.

In addition, our work shows that DHS and its components conducted risk assessments across a number of areas, but should strengthen these assessments. For example, with regard to surface transportation security, in February 2009 we reported that DHS had conducted threat assessments of the commercial vehicle sector and was in the early stages of conducting vulnerability assessments for this sector. However, we reported that TSA's commercial vehicle threat assessments generally did not identify the likelihood of specific threats, as directed by the *National Infrastructure Protection Plan*, and that TSA had not yet determined the scope, method, and time frame for completing vulnerability assessments. We also noted that TSA had not yet conducted consequence assessments, and as a result, could not be sure that its approach for securing the commercial vehicle sector addressed the highest priority security needs. Moreover, in January 2009 we reported that federal entities, including DHS, had efforts underway to assess threat, vulnerability, and consequence for highway infrastructure, but these efforts were not systematically coordinated among key federal partners and the results were not routinely shared. In August 2010, we further reported that TSA developed a pipeline risk assessment model that combined threat, vulnerability, and consequence to create a risk score for each system. However, we reported that DHS should improve the model's consequence component to take account of additional impacts from a possible pipeline attack, such as public health and safety, as called for in the *National Infrastructure Protection Plan*.

Among other things, we recommended that DHS establish a plan and time frames for conducting commercial vehicle sector risk assessments, to include vulnerability and consequence assessments; establish a mechanism to coordinate risk assessment activities and share results related to highway infrastructure; and develop a plan for improving data in the pipeline risk assessment model to include, for example, more data on the consequence component. TSA generally concurred and took action to address them. For example, in 2010 TSA began conducting vulnerability assessments of significant highway bridges under contract with the U.S. Army Corps of Engineers; submitted to Congress assessments required under the Implementing Recommendations of the 9/11 Commission Act

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00884 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.510

of 2007, such as those for the trucking and school bus industries;[5] and developed assessments for highway infrastructure, bus, commercial truck, and port interfaces that were incorporated into the *Transportation Sector Security Risk Assessment*. Moreover, in July 2011 TSA reported that it added data columns for consequence and vulnerability components in its pipeline risk ranking tool to address pipelines in highly populated and high consequence areas. These are important actions that should strengthen TSA's risk assessment efforts across the transportation modes. We have not yet assessed these efforts, and thus cannot make an assessment of TSA's efforts.

In addition, with regard to maritime security, the Coast Guard developed a risk assessment model, the Maritime Security Risk Analysis Model, to assess risk across ports. In April 2010, we reported that the Coast Guard had assessed the risks to cruise ships and facilities using this model. However, our work has shown that the Coast Guard has used the model to assess offshore energy facilities, but faces challenges in doing assessments because of difficulties in determining the types of attack scenarios that could cause significant consequences, and in calculating secondary economic effects. In July 2011, the Coast Guard reported that it is working to improve the accuracy, utility, and standardization of its model, as the modeling, simulation, and analysis of terror attack scenarios improves. We are currently conducting work examining the Maritime Security Risk Analysis Model as well as the extent to which DHS is allocating port security resources based on risk.[6] We plan to report the results from this work later this year.

DHS and its components have taken steps to conduct risk assessments, but they have not always incorporated risk information into their planning and investment decision-making. For example, in July 2010 DHS issued a report on the results of its Bottom-Up Review (BUR) to align DHS's programmatic activities, such as investigating drug smuggling, and its organizational structure to the missions and goals identified in the QHSR.[7] The BUR report identified priority initiatives, such as enhancing

[5] Pub. L. No. 110-53, §§ 1538, 1540(b), 121 Stat. 266, 467, 468 (2007).

[6] We are conducting our work for the Senate committees on Commerce, Science and Transportation Homeland Security and Governmental Affairs, and the House Subcommittee on Border and Maritime Security.

[7] DHS, *Bottom-Up Review Report* (Washington, D.C.: July 2010).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00885 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.511

the department's risk management capability, to strengthen DHS's mission performance, improve departmental management, and increase accountability. In our ongoing review of DHS's QHSR, we found that DHS considered various factors in identifying high priority BUR initiatives for implementation in fiscal year 2012, but did not include risk information as one of these factors. Consideration of risk information could help strengthen DHS's prioritization of mechanisms for implementing the QHSR, including determining which BUR initiatives could be implemented in the short or longer term, and the resources required for implementation. We plan to report on the final results of this work later this year.

Also, with regard to transportation security, DHS has not fully utilized risk information in its strategic planning and prioritization efforts. For example, in March 2009 we reported that TSA had developed an approach to prioritization of its security activities based primarily on intelligence instead of comprehensive risk assessments. We reported that DHS had not reviewed or validated the methodology for this approach; thus, TSA lacked assurance that its approach provided the information needed to guide investment decisions to ensure resources were allocated to the highest risks. Further, with regard to planning efforts, in October 2009, we reported that TSA's strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies was not risk-based. We noted that lacking such information, DHS could not provide reasonable assurance that its strategy was effectively addressing security gaps, prioritizing investments based on risk, and targeting resources toward security measures that would have the greatest impact. Among other things, we recommended that DHS conduct a complete risk assessment related to TSA's passenger screening program and incorporate the results into the program's strategy. DHS generally concurred and reported actions underway to address them. For example, in July 2011, TSA reported beginning to use a risk management analysis process to analyze the effectiveness and efficiency of potential countermeasures and impact on the commercial aviation system. While these are positive steps, it is too early to assess the extent to which they will improve DHS's use of risk information in strategic planning and investment decision making.

GAO Contact

For additional information about this area, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00886 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.512

Appendix XVI: Information Sharing

What This Area Includes

Since September 11, 2001, terrorist threats and attempted attacks have emphasized the importance of developing a national information sharing capability to efficiently and expeditiously gather, analyze, and disseminate terrorism-related information, such as law enforcement, homeland security, and public safety information. The Department of Homeland Security (DHS) has responsibility for sharing terrorism-related information as appropriate with its state and local partners. In 2005, we designated information sharing for homeland security as high risk because the government faced serious challenges in analyzing information and sharing it among federal, state, local, and other security partners in a timely, accurate, and useful way to protect against terrorist threats. We have further reported that DHS must effectively share terrorism-related information with state and local law enforcement because they depend on it to maintain awareness of emerging threats and to allocate homeland security resources, among other things. Further, gaps in sharing, such as agencies' failure to link information about the individual who attempted the December 25, 2009, airline bombing, prevented him from being included on the federal government's terrorist watchlist, a tool used by DHS to screen for persons who pose a security risk.

For the purposes of this report, we are generally highlighting examples of key DHS areas related to information sharing on which we have recently reported and not on areas on which we have not reported or conducted limited audit work. Our work has focused primarily on the sharing of terrorism-related information to identify threats and help prevent terrorist incidents. DHS has other ongoing efforts related to information sharing on which we are not reporting, such as information sharing with the government of Canada for emergency management purposes. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

In our February 2011 high-risk update, as well as a July 2011 report, we reported that the government continued to make progress in sharing terrorism-related information among its many security partners, but did not yet have a fully-functioning Information Sharing Environment in place. This environment is an approach intended to facilitate the sharing of terrorism-related information. Specifically, we reported that the Program Manager for the Information Sharing Environment, as well as key security agencies, including DHS, made progress in implementing a discrete set of goals and activities, and are working to establish an "end state vision" that could help better define what the environment is intended to achieve and include. However, these actions have not yet resulted in a fully

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00887 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.513

functioning environment, and the Program Manager and agencies have not yet identified the incremental costs necessary to implement it or addressed our 2008 recommendation to develop procedures for determining what work remains. DHS is one of the five federal agencies with responsibility for implementing the Environment, and has the lead for sharing information with state, local, tribal, territorial, and private sector partners. Related to this responsibility, DHS has been implementing its information sharing policy and governance structure to improve how it collects, analyzes, and shares homeland security information across the department and with these state and local partners.[1]

DHS expanded and enhanced its sharing of information, but should improve its assistance and services to state and local homeland security partners and streamline some of its information sharing mechanisms. In January 2011, DHS issued a plan for addressing the areas for which it has responsibility under the terrorism-related information sharing high-risk area. DHS identified strategies and initiatives it had planned or underway to address our high-risk criteria and outcomes we identified as important to successfully managing risks that exist due to gaps in information sharing. For example, the plan discussed steps for developing a governance structure for information sharing and beginning efforts to develop a set of metrics for measuring information sharing performance and results. We provided DHS with feedback on this plan. Among other things, we noted the department needs to move toward a system where it accounts for information sharing initiatives against a baseline set of defined capabilities—such as information sharing mechanisms, personnel, and technology—that are needed, to help decision makers weigh progress achieved and remaining to inform investments. Subsequent to our feedback, in July 2011, DHS reported that it had established performance measures for assessing its information sharing efforts. These measures include, for example, the percent of intelligence reports customers rated as "satisfactory" in enabling customers to anticipate emergency threats. DHS plans to report on these metrics beginning in fiscal year 2012. While these are positive steps, our work has shown that developing outcome-based performance measures that gauge information sharing efforts and results would strengthen accountability for these efforts.

[1] DHS has established an Information Sharing Governance Board to identify information sharing priorities, monitor progress in meeting milestones as priorities are identified, and provide assistance as needed.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00888 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.514

Specific to its mission to share information with state and local partners, in December 2010 we reported that DHS's Office of Intelligence and Analysis had initiatives underway to identify these partners' information needs and obtain feedback on intelligence products. The office determined information needs—which are owned and controlled by the states—for 9 of the 50 states and was working with the remaining states to identify their needs.[2] However, we reported that the Office of Intelligence and Analysis had not established mutually agreed upon milestones for completing this effort. We also reported that in addition to intelligence products, the office provided a number of other services to its state and local partners—primarily through these partners' fusion centers where homeland security, terrorism, and intelligence information is shared—that had generally been well received by the center officials we contacted. For example, the Office of Intelligence and Analysis deployed more than 60 intelligence officers to fusion centers nationwide to assist state and local partners in areas such as obtaining relevant intelligence products and leveraging DHS capabilities to support their homeland security missions. However, the office had not yet defined how it planned to meet its state and local information-sharing mission by identifying and documenting the specific programs and activities that are most important for executing this mission. Moreover, its performance measures did not allow the office to demonstrate the expected outcomes and effectiveness of programs and activities that support state and local partners.

We recommended that DHS's Office of Intelligence and Analysis establish milestones for identifying the information needs of state and local partners, identify and document priority programs and activities related to its state and local mission, and establish time frames for developing additional related performance measures. DHS concurred and, as of July 2011, reported determining information needs with 26 of 50 states and working to finalize the others. The Office of Intelligence and Analysis also issued a strategic plan in February 2011 that identified goals, objectives, and performance measures for the office's functions. Further, in July 2011, DHS reported that it was developing a guidebook to explain the process that state and major urban area fusion centers should follow to use customer engagement for identifying, documenting, and prioritizing their intelligence questions, information needs, information

[2] In this context, information needs refer to any general or specific subject for which a state or local agency has a continuing need for intelligence.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00889 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.515

gaps, and collection requirements. According to DHS, this guidebook will help fusion centers identify and document a more accurate and actionable set of information needs and gaps. These actions should help DHS better assess the performance of its information sharing activities. However, it is too early to assess possible results, since they have only recently been, or are in the process of being, implemented.

Moreover, in September 2010 we reported that since 2001, all 50 states and some major urban areas established fusion centers—totaling 72 centers as of July 2011, according to DHS. These centers have cited DHS grant funding as critical to achieving baseline capabilities—the standards the government and fusion centers have defined as necessary for centers to be considered capable of performing basic functions. To provide data about the baseline capabilities of fusion centers nationwide, DHS and other agencies are conducting an ongoing systematic assessment of fusion centers' capabilities. According to DHS senior officials and fusion center representatives, the results of the assessment are intended to provide centers with the information needed to develop more accurate and specific investment justifications. However, DHS had not set standard performance measures for the centers. We recommended that DHS define the steps it will take to design and implement such a set of measures and commit to a target timeframe for completing them. DHS concurred and stated that it has started to develop a framework to demonstrate the value and impact of the national network of fusion centers, and is using nationwide assessment data to support the development of specific performance measures. These efforts should help DHS strengthen its assessment of fusion centers' performance, but it is too soon to assess results as DHS is in the process of implementing these efforts. As we have reported, if centers are to receive continued federal financial support, it is important that they are also able to demonstrate their impact and value added to the nation's information sharing goals.

Additionally, we have reported that DHS and the Transportation Security Administration (TSA) have taken steps to share surface transportation security information with stakeholders in different sectors. For example, DHS established the Homeland Security Information Network, which was designed to serve as the department's primary information-sharing mechanism for the larger homeland security community engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents under DHS jurisdiction. Within the Homeland Security Information Network, each of the 18 critical infrastructure sectors maintains its own site, and under the transportation

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00890 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.516

sector, there are sites for different transportation modes, such as public transit. We found in September 2010 that 75 percent of the public transit agencies we surveyed reported being generally satisfied with the security-related information they received.

However, we have identified several challenges to DHS's information sharing efforts for surface transportation security. For example, some public transit agencies cited the need to streamline the information they received, and we identified the potential for overlap between the Public Transportation Information Sharing and Analysis Center,[3] the Public Transit Portal of DHS's Homeland Security Information Network, and the Transportation Security Information Sharing and Analysis Center,[4] which all communicate similar unclassified and security-related information to public transit agencies. Also, preliminary observations from interviews and open-ended responses to a survey as part of our ongoing work indicate that some freight rail stakeholders would prefer to receive more analysis or actionable information from TSA, such as trend analysis of incidents or suggestions for improving security arrangements, that could help predict how certain events may affect rail systems.[5] In addition, DHS and TSA have not developed performance goals and outcome-oriented measures to gauge the effectiveness of their information-sharing networks.

We recommended that DHS establish time frames for a working group of federal and industry officials to assess opportunities to streamline information-sharing mechanisms to reduce any unneeded overlap, and for developing goals and related outcome-oriented performance measures specific to each security information network. DHS concurred, and TSA and industry groups developed a report and associated library, which is intended to streamline the analysis, sharing, and exchange of

[3] The Public Transportation Information Sharing and Analysis Center, which is implemented by the American Public Transportation Association and funded by TSA, collects, analyzes, and distributes security and threat information from the federal government and open sources on a 24/7 basis.

[4] TSA's Office of Intelligence implemented its page on the Homeland Security Information Network in March 2010 as a collaborative information-sharing platform for all transportation modes, including public transit.

[5] This work is being conducted in response to a mandate in the Implementing Recommendations of the 9/11 Commission Act of 2007. Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007). We plan to issue our findings on this work later this year.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00891 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.517

intelligence and security information that had been disseminated by multiple sources. Further, in July 2011 TSA reported that it and key industry groups were engaged in an ongoing process to develop, improve, and refine its information sharing mechanisms. In addition, TSA reported that it continues to work with its stakeholders to determine how available intelligence and other security incident data can be leveraged to provide stakeholders with meaningful information to help guide actions in the field. We are continuing to assess TSA's efforts related to sharing security information with stakeholders in the aviation, rail, and highway modes and will report the final results later this year.

GAO Contact

For additional information about this area, contact Eileen Larence at (202) 512-6510 or larencee@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00892 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.518

Appendix XVII: Partnerships and Coordination

What This Area Includes

The Department of Homeland Security (DHS) provides federal leadership for homeland security, but also plays a large role in coordinating the homeland security activities of other federal, state, local, private sector, and international stakeholders. We reported that successful partnering and coordination involves collaborating and consulting with stakeholders to develop and agree on goals, strategies, and roles to achieve a common purpose; identify resource needs; establish a means to operate across agency boundaries, such as compatible procedures, measures, data, and systems; and agree upon and document mechanisms to monitor, evaluate, and report to the public on the results of joint efforts. If these entities do not effectively coordinate their implementation activities, they may waste resources by creating ineffective and incompatible pieces of a larger security program. For example, because the private sector owns or operates a majority of the nation's critical infrastructure, DHS must partner with individual companies and sector organizations to protect vital national infrastructure, such as the nation's water supply, transportation systems, and chemical facilities.

For the purposes of this report, we are generally highlighting examples of key DHS areas related to partnerships and coordination on which we have recently reported. We are generally not addressing areas on which we have not reported or have conducted limited audit work. For example, DHS has ongoing efforts related to coordinating with homeland security partners within and across its various mission areas and programs, such as for combating nuclear terrorism and conducting biological research to support the nation's biodefense preparedness. We have not completed work on these areas upon which to make an assessment of DHS's progress.

Key Progress and Work Remaining

DHS made progress in coordinating its programs and activities with homeland security partners, but should strengthen its coordination by, among other things, better meeting the information needs of private sector partners and providing oversight of coordination mechanisms. DHS has strengthened its coordination with homeland security partners in a number of functional areas, such as aviation security, critical infrastructure protection, border security, and emergency preparedness and response, but should further enhance coordination efforts. For example, with regard to aviation security, in December 2010, we reported that DHS and the Transportation Security Administration (TSA) worked on coordinating security standards and practices to enhance security with foreign partners—a process known as harmonization. DHS and TSA did so through increased global outreach,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00893 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.519

coordination of standards and practices, use of enhanced technology, and assessments of foreign airports. We also reported that DHS and TSA coordinated with foreign governments to harmonize air cargo security practices to address the statutory mandate to screen 100 percent of air cargo transported on U.S.-bound passenger aircraft.[1] In July 2011, TSA reported that it had requested air carrier feedback on their ability to accomplish 100 percent of screening on international inbound air cargo by December 2011, and is evaluating industry comments to finalize its strategy and establish a feasible timeline for implementing the screening requirement.

With regard to critical infrastructure protection, in September 2010 we reported that DHS's National Protection and Programs Directorate (NPPD) operates the Protective Security Advisor Program, which deploys critical infrastructure protection and security specialists, called Protective Security Advisors, to local communities throughout the country. These advisors lead NPPD's efforts in these locations and act as a link between state, local, tribal, and territorial organizations and DHS infrastructure mission partners. DHS also reported that these advisors work to maintain relationships with the private sector and local communities to help foster effective information sharing and disseminate information to the private sector during times of increased threat.

Further, in July 2010 we reported on the expectations of public and private sector stakeholders for their cyber-related public-private partnerships. The expectations that the partners identified included timely and actionable cyber-threat information and alerts and a single centralized government cybersecurity organization to coordinate government efforts. Federal partners, including DHS, took steps to help address the expectations of the private sector, including developing new information-sharing arrangements and expanding the number of private sector individuals with security clearances. However, much work remains in ensuring that the expectations of public and private stakeholders are fully met. For example, less than one-third of private sector respondents reported that they were receiving actionable cyber threat information and alerts from federal partners to a great or moderate extent. We recommended that DHS work with its federal and private sector partners to enhance information-sharing efforts. DHS concurred and reported in

[1] See 49 U.S.C. § 44901(g).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00894 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.520

July 2011 that it was taking additional action by, for example, establishing cybersecurity working groups, interagency coordination groups, and a performance measure for fiscal year 2012 to seek public and private sector feedback on the extent to which DHS cybersecurity products are actionable and timely. However, as DHS is in the processing of implementing these efforts, it is too early to assess their effectiveness.

With regard to border security, in December 2010 we reported that federal, state, local, tribal, and Canadian law enforcement partners reported improved DHS coordination to secure the northern border. For example, interagency forums helped establish a common understanding of border security threats, while joint operations helped to achieve an integrated and effective law enforcement response. However, challenges remained in sharing information and resources useful for operations along the northern border. For example, partners in all four sectors we visited cited ongoing challenges in sharing information and resources for daily border security-related to operations and investigations, and we reported that oversight by management at the component and local level had not ensured consistent compliance with provisions of interagency agreements, such as those related to information sharing.[2] In November 2010, we reported that information sharing and communication among the Departments of Agriculture, Homeland Security, and Interior for securing federal and tribal lands along the border had increased, but that critical gaps remained. For example, these agencies had established forums and liaisons to exchange information; however, in one sector they did not coordinate to ensure that federal land law enforcement officials maintained access to threat information and compatible secure radio communications for daily operations. Coordination in these areas could better ensure officer safety and an efficient law enforcement response to illegal activity.

Moreover, we reported in February 2008 that the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program office, which is to verify the identities of foreign visitors entering and exiting the United States by storing and processing biometric and biographic information, had not fully defined its relationships with other immigration

[2] We visited the Blaine, Spokane, Detroit, and Swanton sectors. While we could not generalize our work from these visits to all locations along the northern border, the information we obtained provided examples of the way in which DHS and other federal agencies coordinated their efforts with northern border partners.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00895 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.521

and border management programs or its approaches relative to addressing outcomes shared by those programs. As a result, we concluded that the department risked suboptimizing how its programs collectively supported its immigration and border management goals and objectives. We have made recommendations to DHS to strengthen its border security coordination efforts. For example, we recommended that DHS provide oversight to ensure efficient use of border security interagency forums and compliance with interagency agreements; take necessary action to ensure that personnel conduct early and continued consultations to coordinate on, among other things, threat information for federal lands that is timely and actionable; and fully define relationships between the US-VISIT program and other programs.

DHS concurred and reported, for example, that it plans to review the inventory of interagency forums through its strategic and operational planning efforts to assess efficiency and identify challenges. Further, in July 2011, the US-VISIT program office reported taking action to coordinate with other immigration and border security programs. For example, it reported that it had established a governance board to enhance border security solutions to meet congressional mandates, and supported the expansion of immigration enforcement related programs, such as Secure Communities through which U.S. Immigration and Customs Enforcement works with state and local law enforcement agencies to identify and remove immigration violators. While these are positive steps, DHS needs to demonstrate that these efforts have helped the department to fully define relationships between the US-VISIT program and other programs.

In addition, with regard to emergency preparedness and response and chemical, biological, radiological, and nuclear incident preparedness, in June 2011 we reported that DHS and the Department of Health and Human Services coordinated with each other and with other federal departments to develop chemical, biological, radiological, and nuclear risk assessments, but neither department had written procedures for developing these assessments. Our best practices for interagency collaboration and federal standards for internal control indicate that agencies can best enhance and sustain coordination by adopting key practices, such as defining desired common outcomes, agreeing on roles and responsibilities, and developing written policies and procedures to help ensure that management directives are enforced. We reported that such practices and standards should help DHS and the Department of Health and Human Services institutionalize their agreements on these sensitive and technical issues to better ensure coordination, collaboration,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00896 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.522

and continuity beyond the tenure of any given official or individual office, and recommended that the departments develop these practices. DHS concurred with our recommendation.

GAO Contact

For additional information about this area, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00897 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.523

Appendix XVIII: Developing and Deploying New Technologies for Homeland Security

What This Area Includes

Since beginning operations in 2003, the Department of Homeland Security (DHS) has spent billions of dollars on research and development of technologies and other countermeasures to address threats and conduct its missions. DHS programs represent hundreds of billions of dollars in life-cycle costs and support a wide range of missions and investments, including border surveillance and screening equipment, nuclear detection equipment, information systems that help detect and interdict the planning of terrorist acts, and technologies used to screen airline passengers and baggage for explosives. Within DHS, the Science and Technology Directorate (S&T) has the authority to coordinate overall research and development efforts to improve homeland security. Among other things, S&T works with DHS components to provide assistance in researching and developing technologies to meet their specific missions, while the components themselves are responsible for developing, testing, and acquiring these technologies. For instance, the Transportation Security Administration (TSA) works with S&T to research, develop, and deploy technologies to, for example, screen airline passengers and their baggage. DHS's Domestic Nuclear Detection Office (DNDO) is responsible for developing, acquiring, and supporting the deployment of programs and systems to detect and report on attempts to develop, transport, or use unauthorized nuclear explosive, fissile, or radiological materials or explosives in the United States.

For the purposes of this report, we are generally highlighting examples of DHS efforts related to developing and deploying new technologies on which we have recently reported, and are generally not addressing areas on which we have not reported or have conducted limited audit work. While this section addresses examples on which we have reported, which focus on DHS's efforts related to technologies for border, transportation, and maritime security, DHS has other efforts related to developing and deploying new technologies, such as technologies for intelligence. DHS also reported that it has taken steps intended to formalize requirements definition and technology development. We have not completed work on these areas upon which to make an assessment of DHS's progress.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00898 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.524

Key Progress and Work Remaining

DHS took action to develop and deploy new technologies to help meet its homeland security missions. However, in some instances DHS pursued acquisitions without ensuring that the technologies met defined requirements and faced challenges in conducting and documenting testing and evaluation and performing cost-benefit analyses. DHS developed and deployed various technologies within its functional areas, including maritime and transportation security. For example, in September 2010, we reported that DHS made progress in researching and developing container security technologies. Specifically, we reported that since fiscal year 2004 DHS conducted research and development for four container security technology projects to monitor cargo tampering and, according to DHS, provide a global communication system to securely transmit information to DHS components responsible for port security. Moreover, in June 2010 we reported that DHS made significant progress in deploying radiation detection equipment to scan cargo and conveyances entering the United States through fixed land and sea ports of entry for nuclear and radiological materials. Specifically, we reported that DHS deployed more than 1,400 radiation portal monitors to ports of entry. Further, TSA continues to deploy technologies to screen checked baggage. As of July 2011, TSA reported that it had about 2,300 explosives detection systems in its fleet, about 1,900 of which were deployed at airports in the United States.[1] At airports and terminals that do not use these systems, explosives trace detection machines are used for primary checked-baggage screening, typically at smaller airports.[2] As of July 2011, TSA estimated that there were about 5,000 explosives trace detection machines used for the primary or secondary screening of checked baggage at U.S. commercial airports. In addition, in June 2010 we reported that DHS, the United States Postal Service, and the Department of Defense developed and implemented technologies to sample the air and test for specific biological agents. In particular, DHS's BioWatch program had been implemented in more than 30 metropolitan areas and tests for the presence of multiple biological agents.

[1] An explosives detection system uses computed tomography technology to automatically measure the physical characteristics of objects in baggage. The system automatically triggers an alarm when objects that exhibit the physical characteristics of explosives are detected.

[2] An explosives trace detection machine is used to chemically analyze trace materials after a human operator swabs checked baggage to identify any traces of explosive material.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00899 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.525

However, our work has shown that DHS made acquisition decisions without ensuring that the systems met program and performance requirements.

- In September 2010, we reported that DNDO was simultaneously engaged in the research and development phase while planning for the acquisition phase of its cargo advanced automated radiography system to detect certain nuclear materials in vehicles and containers at ports. DNDO pursued the acquisition and deployment of the cargo advanced automated radiography system without fully understanding that it would not fit within existing inspection lanes at ports of entry. This occurred because, during the first year or more of the program, DNDO and U.S. Customs and Border Protection (CBP) had few discussions about operating requirements for primary inspection lanes at ports of entry. DHS announced the termination of the program in 2010.
- In July 2011, we reported that TSA revised its explosives detection system requirements to better address current threats in screening checked baggage, and plans to implement these requirements in a phased approach. However, we reported that some number of systems in TSA's fleet was configured to detect explosives at the levels established in the 2005 requirements and that the remaining systems were configured to detect explosives at 1998 levels. When TSA established the 2005 requirements, it did not have a plan with time frames to deploy the explosives detection systems to meet the new requirements. We recommended that TSA develop a plan to deploy and operate explosives detection systems to meet the most recent requirements. TSA concurred and, in July 2011, reported that it intends to finalize a plan by the fourth quarter of fiscal year 2012.

DHS also encountered challenges in conducting and documenting testing and evaluation of its technologies. Our prior work identified that the failure to resolve problems discovered during testing can sometimes lead to costly redesign and rework at a later date, and that addressing such problems during the testing and evaluation phase before acquiring systems can help agencies avoid future cost overruns. For example:

- In June 2011 we reported that S&T's Test & Evaluation and Standards Office, responsible for overseeing test and evaluation of DHS's major acquisition programs, reviewed or approved test and evaluation documents and plans for programs undergoing testing, and conducted independent assessments for the programs that completed operational testing. DHS senior level officials considered the office's assessments and input in deciding whether programs were ready to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00900 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.526

proceed to the next acquisition phase. However, the office did not consistently document its review and approval of components' test agents—a government entity or independent contractor carrying out independent operational testing for a major acquisition. In addition, the office did not document its review of other component acquisition documents, such as those establishing programs' operational requirements.

- In March 2011, we reported that the independent testing and evaluation of the Secure Border Initiative Network's virtual fence Block 1 capability to determine its operational effectiveness and suitability was not complete at the time DHS reached its decision regarding the future of the Secure Border Initiative Network, or requested fiscal year 2012 funding to deploy the new Alternative (Southwest) Border Technology.[3] We reported that because the new Alternative (Southwest) Border Technology incorporates a mix of technology that includes an Integrated Fixed Tower surveillance system similar to that currently used in the Secure Border Initiative Network, such testing and evaluation could have informed DHS's decision about moving forward with the new technology deployment.
- In September 2010, we reported that S&T's master plans for conducting operational testing of container security technologies did not reflect all of the operational scenarios that CBP was considering for implementation. For example, S&T did not include certain scenarios necessary to test how a cargo container would be transported throughout the maritime supply chain. Until the container security technologies are tested and evaluated consistent with all of the operational scenarios, S&T cannot provide reasonable assurance that the technologies will function as intended.

We recommended, among other things, that S&T develop mechanisms to document its review of component acquisition documentation, and that DHS test and evaluate the container security technologies consistent with all of the operational scenarios DHS identified for potential implementation. DHS concurred and reported actions underway to address them, such as drafting a memorandum on the document review

[3] Secure Border Initiative Network Block 1 is a surveillance, command, control, communications, and intelligence system fielded in parts of Arizona that is intended to mitigate or eliminate vulnerabilities along the international border between ports of entry. Block 1 is an element of DHS's Secure Border Initiative, a comprehensive, multiyear plan to secure the borders of the United States and reduce illegal cross border activities such as smuggling of economic migrants, illegal drugs, and people with terrorist intent.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00901 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.527

process. Further, in July 2011, S&T and CBP reported starting a joint pilot program to implement a new supply chain security technology on selected rail and truck cargo routes from Mexico and Canada into the United States to evaluate land cargo security devices intended to monitor unauthorized door openings or anomalies and to provide encrypted in-transit tracking.

In addition, DHS has not consistently included cost-benefit analyses in its acquisition decision making. Our prior work shows that cost-benefit analyses help decision makers assess and prioritize resource investments and consider potentially more cost-effective alternatives. For example, in 2006, we recommended that DHS's decision to deploy next-generation radiation-detection equipment, or advanced spectroscopic portals, used to detect smuggled nuclear or radiological materials, be based on an analysis of both the benefits and costs and a determination of whether any additional detection capability provided by the portals was worth their additional cost.[4] DHS subsequently issued a cost-benefit analysis, but we reported that this analysis did not provide a sound analytical basis for DHS's decision to deploy the portals. In June 2009, we also reported that an updated cost-benefit analysis might show that DNDO's plan to replace existing equipment with advanced spectroscopic portals was not justified, particularly given the marginal improvement in detection of certain nuclear materials required of advanced spectroscopic portals and the potential to improve the current-generation portal monitors' sensitivity to nuclear materials, most likely at a lower cost. At that time, DNDO officials stated that they planned to update the cost-benefit analysis. In July 2011, DHS announced that DNDO and CBP would end the advanced spectroscopic portal project as originally conceived given the challenges the program faced. DHS reported that it plans to deploy the existing units to field locations to gather operational data to support future planning efforts.

In June 2011, DHS reported that it is strengthening its investment and acquisition management processes across the department by implementing a decision-making process at critical phases throughout the investment life cycle. For example, DHS reported that it plans to establish a new model for managing departmentwide investments across their life cycles. Under this plan, S&T would be involved in each phase of the

[4] We later estimated these costs to be over $2 billion.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00902 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.528

investment life cycle and participate in new councils and boards DHS is planning to create to help ensure that test and evaluation methods are appropriately considered as part of DHS's overall research and development investment strategies. In addition, DHS reported that the new councils and boards it is planning to establish would be responsible for, among other things, making decisions on research and development initiatives based on factors such as viability and affordability, and overseeing key acquisition decisions for major programs using baseline and actual data. According to DHS, S&T will help ensure that new technologies are properly scoped, developed, and tested before being implemented. In July 2011, S&T reported that it established a new group to work with DHS components to, among other things, help ensure that operational requirements are completely specified and validated and that comprehensive cost-benefit analyses are performed to identify the best alternative for meeting identified mission needs. However, as DHS has recently established this group, it is too soon to assess its effectiveness. DHS also reports that it is working with components to improve the quality and accuracy of cost estimates and increased its staff during fiscal year 2011 to develop independent cost estimates, a best practice, to ensure the accuracy and credibility of program costs. DHS reports that four cost estimates for level 1 programs have been validated to date.[5] The actions DHS reported taking or underway to address the management of its acquisitions and the development of new technologies are positive steps and, if implemented effectively, could help the department address a number of these challenges.

GAO Contact

For additional information about this area, contact David Maurer at (202) 512-9627 or maurerd@gao.gov.

[5] Levels are determined by the life-cycle cost of the program, not the procurement cost. Level 1 (major acquisition) life-cycle cost is identified at or above $1 billion dollars.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00903 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.529

Appendix XIX: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 31, 2011

Cathleen A. Berrick
Managing Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-11-881, "DEPARTMENT OF HOMELAND SECURITY: Progress Made and Work Remaining in Implementing Homeland Security Missions Ten Years after 9/11"

Dear Ms. Berrick:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report. The Department concurs with GAO's conclusion that "Eight years after its establishment and 10 years after the September 11, 2001, terrorist attacks, DHS has indeed made significant strides in protecting the nation ...". As described in the DHS progress report on fulfilling 9/11 Commission recommendations[1], released by Secretary of Homeland Security Janet Napolitano in July 2011, America is a stronger, safer and more resilient country because of the work DHS and its many partners do every day.

A Changed Security Environment

Following the terrorist attacks of September 11, 2001, Congress moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, local, tribal, and territorial capabilities to prepare for, respond to, and recover from threats and disasters at home. A key element of Congress's vision for a new security framework included the creation of DHS in March 2003, bringing together 22 separate agencies and offices into a single, Cabinet-level department.

[1] DHS. *Implementing 9/11 Commission Recommendations: Progress Report 2011.* http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf

1

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00904 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.530

Since its inception, DHS has made significant progress in securing the nation from terrorism. Comparing today's security architecture to what existed in 2001 illustrates how far we have come in making the country safer and more secure today than it was a decade ago. The following examples highlight a few of the Department's many accomplishments:

Visa Security: Since 2001, DHS has created and managed the Visa Security Program, which is now operational at 19 posts in 15 countries. Through this program, Immigration and Customs Enforcement deploys trained special agents overseas to high-risk visa activity posts to conduct targeted, in-depth reviews of particular visa applications and applicants before they reach the United States.

Border Security: Since 2001, the Department has deployed unprecedented levels of personnel, technology, and resources to the Nation's borders. DHS has increased the number of civilian boots on the ground from approximately 9,800 Border Patrol agents in 2001 to more than 20,800 today.

Fusion Centers: Since 2001, 72 fusion centers have been created to serve as focal points for the receipt, analysis, gathering, and sharing of threat and vulnerability-related information. DHS has provided personnel, grant funding, technical assistance, security clearances, and access to classified networks to help fusion centers achieve and maintain critical operational capabilities. These fusion centers allow the Intelligence Community to identify the common threads that can tie a seemingly minor crime to the larger threat picture, an essential capability that was not in existence just ten years ago.

Passenger Screening and Prescreening: Since 2001, DHS has developed the capacity to prescreen 100 percent of the 14 million passengers flying weekly to, from, and within the U.S. against government watch lists, enabling the Department to identify individuals who are on the "No Fly" list and recommend others for additional screening. Ten years ago, screening of passengers coming to the United States was limited to the visa process and inspection of a person by an immigration officer at the port of entry. Additionally, the Transportation Security Administration (TSA) has deployed roughly 50,000 Transportation Security Officers at more than 450 airports nationwide. TSA has also accelerated the deployment of new technologies to detect the next generation of threats.

In-flight Security: Since 2001, Federal Air Marshals have greatly increased in number, from 33 to thousands in 2011, and are now deployed across the aviation system based on risk. The Federal Flight Deck Officer program allows qualified pilots to use firearms to defend the cockpit and TSA runs a crewmember behavior recognition and response training program. Additionally, the hardening of cockpit doors prevents unauthorized access to the flight deck. Over the past ten years, these efforts have significantly enhanced the safety and security of passengers on board.

Surface Transportation Security: Since 2001, DHS has strengthened efforts in the surface domain to reduce security vulnerabilities and to strengthen resilience against terrorist attacks. For example, DHS has deployed 25 Visible Intermodal Prevention and Response (VIPR) Teams to protect surface transportation, provide deterrent and

2

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00905 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.531

detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities.

International Information Sharing: Since 2001, eighteen countries have joined the United States to share information about terrorists and criminals to prevent them from traveling freely between countries.

Chemical, Biological, Radiological, and Nuclear (CBRN) Threats: Since 2001, DHS has made significant progress in assessing risks posed by CBRN threats and developing and deploying capabilities to detect and mitigate those threats. From BioWatch to an interagency-approved Global Nuclear Detection Architecture Strategic Plan, the Department is systemically addressing the needs of the Nation to reduce the threat of CBRN terrorism. The Department appreciates GAO's acknowledgement that "DHS made progress in assessing risks posed by CBRN threats."

Emergency Communications: Since 2001, FEMA has continued to support state, local, tribal, and territorial partners' efforts to enhance their emergency communications capabilities through grants and technical assistance. Additionally, in July 2008, DHS issued the National Emergency Communications Plan—the first strategic document for improving emergency communications nationwide.

Not only has the Department made significant progress in securing the Nation from terrorism, it also has achieved measurable success developing a Nation that is resilient to natural disasters and threats of all kind. The Department appreciates GAO's acknowledgement that DHS "expanded its efforts to improve national emergency preparedness and response planning; improved its emergency assistance services; supported state, local, and tribal partners' disaster response capabilities; and enhanced emergency communications."

A Strategic View of Homeland Security

In February 2010, DHS issued its first Quadrennial Homeland Security Review (QHSR) report, outlining a strategic framework for homeland security to guide the activities of the Department and its homeland security partners, including federal, state, local, tribal, and territorial government agencies; the private sector; and nongovernmental organizations.[2] The report identified five homeland security missions—Preventing Terrorism and Enhancing Security; Securing and Managing Our Borders; Enforcing and Administering Our Immigration Laws; Safeguarding and Securing Cyberspace; and Ensuring Resilience to Disasters—and goals and objectives to be achieved within each mission. The report also identifies goals and objectives for maturing and strengthening the homeland security enterprise.

This first QHSR report has set the stage for detailed analyses of homeland security capabilities and requirements. This report will drive Department progress by redefining the homeland security missions and setting prioritized goals, objectives, and strategic outcome statements for each mission, and guiding all homeland security stakeholders toward common

[2] DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, D.C.: February 2010).

3

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00906 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.532

goals and objectives. A coordinated approach that promotes unity of effort will provide the foundation to combat current, emerging, and future threats to the homeland.

The Department appreciates GAO's willingness to align its report to the five new homeland security missions identified in the QHSR.

Report's Limited Scope

DHS acknowledges GAO's work documenting the progress the Department has made in enhancing the nation's security and the challenges that still exist. However, as GAO states, the report "does not address . . .all of DHS's homeland security-related activities and efforts." Additionally, as GAO notes, its assessments of the progress in each area is not comprehensive because GAO and the DHS Office of Inspector General (OIG) have completed varying degrees of work for each of the ten functional areas discussed in the report.

In fact, there are a number of DHS activities not reflected in the GAO report that demonstrate progress the Department has made in preparing the nation for threats. For example, the report does not acknowledge certain DHS programs, such as the Western Hemisphere Travel Initiative (WHTI), which have improved security to the United States. WHTI imposes secure identity and citizenship documentation requirements, and its implementation has significantly expedited legitimate travel through improved Port of Entry processing. The report also does not mention some of the improvements resulting from the Department's increased coordination across the Federal government, as exemplified by the analysis of travel-related data. While watch lists existed prior to 9/11, they were neither coordinated nor consolidated to the degree and depth that they are now. Today, four centers across the Federal government provide information regarding potential terrorist travel: the Federal Bureau of Investigation's Terrorist Screening Center, National Counterterrorism Center, the National Targeting Center, and the Human Smuggling and Trafficking Center. For additional information on other key areas of progress, see the Department's recently released report that highlights progress fulfilling specific 9/11 Commission recommendations.[3]

Continuing Work with GAO

DHS senior leadership, including the Secretary and Deputy Secretary, have demonstrated a strong and continuing commitment to building and strengthening the Department's relationship with GAO in a mutually beneficial and productive manner. DHS has worked vigorously to close out recommendations from the GAO and OIG, and has made notable progress. In fact, DHS recently developed a strategic framework to manage risk and detailed corrective action plans to address each one of GAO's high risk recommendations. Last year, Secretary Napolitano also signed a Management Directive on relations between DHS and GAO concerning statutorily authorized GAO reviews of DHS activities. The new Directive played an essential role during this engagement as subject matter experts from across the Department worked to provide updated information and documentation to their GAO counterparts. The Department appreciates GAO's receptiveness to our input, and looks forward to continuing our dialogue to further enhance GAO's understanding of all DHS has done and is currently doing to make America a stronger, safer and more resilient nation.

[3] DHS. *Implementing 9/11 Commission Recommendations: Progress Report 2011.* http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf

4

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00907 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.533

Again, thank you for the opportunity to review and comment on this draft report. I look forward to working with you on future Homeland Security issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

5

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00908 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.534

Appendix XX: GAO Contact and Staff Acknowledgments

GAO Contact

Cathleen A. Berrick (202) 512-3404 or berrickc@gao.gov

Staff Acknowledgments

In addition to the person named above, Rebecca Gambler, Assistant Director; Taylor Matheson, Analyst-in-Charge; Melissa Bogar; Susan Czachor; Lorraine Ettaro; Sarah Kaczmarek; Tracey King; Dawn Locke; Jan Montgomery; Jessica Orr; and Meghan Squires made key contributions to this report. Other contributors to this report included Joel Aldape; David Alexander; Gene Aloise; Rodell Anderson; Aditi Archer; Sarah Arnett; Neil Asaba; Ben Atwater; Jonathan Bachman; Charles Bausell; Claudia Becker; Scott Behen; Carolyn Blocker; David Bruno; Carissa Bryant; Rochelle Burns; Alicia Cackley; Stephen Caldwell; Lisa Canini; Caitlin Carlberg; Tammy Conquest; Christopher Currie; Ryan Consaul; Frances Cook; Joseph Cruz; Anthony DeFrank; Davi D'Agostino; Kay Daly; Deborah Davis; Katherine Davis; Vanessa Dillard; Michael Dino; Rick Eiserman; Eric Erdman; Jeanette Espinola; Alana Finley; Edward George; Robin Ghertner; Michael Gilmore; Kathryn Godfrey; Robert Goldenkoff; Mark Goldstein; Barbara Guffy; Geoffrey Hamilton; Christopher Hatscher; Brent Helt; David Hinchman; Richard Hung; John Hutton; William O. Jenkins, Jr.; Amanda Jones; Yvonne Jones; Valerie Kasindi; Christopher Keisling; Anjalique Lawrence; Michael Lenington; Eileen Larence; Marya Link; Thomas Lombardi; Stephen Lord; Robert Lowthian; Jessica Lucas Judy; David Lysy; Gary Malavenda; Kush Malhotra; David Maurer; Linda Miller; Lara Miklozek; Anthony Moran; Steve Morris; John Mortin; Gary Mountjoy; Suzanne Murphy; Robin Nye; Jean Orland; Sabine Paul; David Powner; Paula Rascona; Janay Sam; Debra Sebastian; Richard M. Stana; Kevin Tarmann; Nathan Tranquilli; Katherine Trimble; Meg Ullengren; Sarah Veale; Gregory Wilshusen; Michelle Woods; and Edwin Woodward.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00909 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.535

Post-Hearing Questions for the Record
Submitted to the Honorable Jane Holl Lute
From Senator Joseph I. Lieberman

"Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security"
September 7, 2011

Question#:	1
Topic:	issues
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Government Accountability Office reports that DHS has made important strides in strengthening its management functions—acquisition, information technology, financial management, and human capital management.

Looking forward, what management-related issues are high priorities for the leadership of the Department and what steps are being taken to address them?

In times of constrained government budgets, management accounts are often targeted for cuts. In your view, how important is management at the Department? What would be the impact of cuts of DHS management accounts, both in the short-term and long-term?

Response: DHS continues to drive a comprehensive, strategic management approach focused on enhancing the people, structures, and processes necessary to effectively and efficiently meet mission goals and support frontline operations. Our approach is designed to integrate and align business functions at the Departmental and Component levels. While we are making improvements in all functional areas, particular emphasis is being made in the following:

1. *Acquisition Management:* DHS is committed to continuing to improve the efficiency and effectiveness of the acquisition process. We are focused on strengthening the "front end" requirements and "back end" program management practices to encourage fiscal responsibility and minimize risk across the acquisition life-cycle.

   The Department's acquisition management framework is growing stronger through the refinement of our policy, processes, procedures, and the placement of people with the right skill sets in program offices. The goal is for every major

67123.536

Question#:	1
Topic:	issues
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

program to be managed by a certified program manager and implemented in the most responsible and efficient manner possible.

We are actively working to strengthen the Integrated Investment Life Cycle Model (IILCM), which will facilitate our ability to excel in all facets of planning, procuring, and managing the execution of our major programs. We have also developed and are preparing to launch AP3EX (Acquisition Portfolio/Program/Project Execution), a business support tool to support the governance of investments across DHS.

2. *Information Technology:* DHS continues to focus on creating a unified information technology infrastructure for effective integration and agency-wide management of IT assets and programs.

   Current DHS programs are Component-centric with minimal Department-level prioritization and alignment with overall strategic and mission objectives. We lack adequate policies and best practices that enable effective oversight and execution of programs, as well as comprehensive strategies for effective future planning at the Department-level.

   To address this challenge, the Department has implemented an IT Program Governance initiative. The purpose of the initiative is to better align and prioritize IT Initiatives and outcomes to our strategic plan, mission objectives, and budget processes; and deliver IT services to customers that meet identified performance, cost and quality measures for programs and projects. We plan to achieve these outcomes by implementing a tiered governance structure based on identified portfolios (as defined in the Enterprise Architecture) to support strategic, mission and tactical delivery of IT programs. We will also integrate governance with the budget planning process, mitigate risks, monitor progress, identify opportunities for increased efficiency, and implement standardized processes across the Department.

3. *Financial Management:* The Department is focused on improving our financial systems and capabilities in both the Management Directorate and the Components.

   DHS has a strong commitment to strengthening Department-wide financial management and last year Secretary Napolitano committed to obtaining an audit opinion on the Department's balance sheet. In FY 2011, the Department met this

67123.537

Question#:	1
Topic:	issues
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

goal and received a qualified opinion on its balance sheet and Statement of Custodial Activity. This is a pivotal step to increasing transparency and accountability and accurately accounting for the Department's resources and is a significant milestone that highlights how we have significantly improved financial management at DHS. Looking forward, to further demonstrate our commitment, we are concentrating our efforts on expanding the scope of our audit to our remaining Statements of Budgetary Resources, Net Cost, and Changes in Net Position in FY 2012. We will continue to ensure taxpayer dollars are managed with integrity, diligence, and accuracy, and that the systems and processes used for all aspects of financial management demonstrate the highest level of accountability and transparency.

4. *Human Capital Management:* Making sure we have the right people in the right positions at the right time, with the proper workforce balance between federal and contract employees remains a priority for the Department.

   DHS is committed to ensuring we have the knowledge, skills, abilities, and diversity to meet our mission goals and objectives. We have developed and are implementing a comprehensive workforce planning strategy to identify current and future human capital needs, as well as ensuring the Department has an appropriately balanced workforce. For example, we have advanced our efforts to increase Veteran and disability hiring and have met Secretary Napolitano's hiring goal of 50,000 veterans a year ahead of schedule. In addition, as of June 2011, we achieved the 2009 in-sourcing initiative goal of eliminating 3,500 contractor positions. In August 2011, we revalidated the Department's Mission Critical Occupations, organized by Quadrennial Homeland Security Review (QHSR) mission areas.

   Moreover, DHS has made progress to improve the effective and efficient management of the Department over the past several years; however, much more needs to be accomplished to address issues highlighted in the Employee Viewpoint Survey, particularly regarding training, education, and employee development opportunities. In order to continue to address these issues, the Department will: 1) design and implement a robust and innovative leader development program that provides all supervisors, managers, and executives with the necessary skills to be effective and efficient leaders; 2) implement coherent succession planning strategies to ensure that it has a "pipeline" of employees ready and capable of assuming positions of increased trust and responsibility; 3) ensure that it has employee development programs that

67123.538

Question#:	1
Topic:	issues
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

incorporate new approaches and maximize existing vehicles required to develop a more diverse and highly capable cadre of future DHS leaders at all levels of the workforce; and 4) per mandate of HR5441 Section 622, continue with implementation of a rotational assignments program to facilitate movement of employees between the DHS operational and support Components. DHS is also leveraging the President's Management Council's interagency rotations program to enhance employee knowledge of the interagency.

In addition, in January 2011 (updated in June 2011), the Under Secretary for Management submitted the Department's first comprehensive Integrated Strategy for High Risk Management to the Government Accountability Office (GAO), covering all functional lines-of-business. The plan provided detailed, specific action items to be addressed by the department to further enhance and improve management operations. GAO has acknowledged that the Department has made "important progress" and should continue to implement the goals set forth in several Corrective Action Plans.

While in the current fiscal environment, the Department's management functions are more important than ever to effectively and efficiently support and coordinate frontline operations, targeted reductions to DHS management accounts have helped preserve funding for these critical operations.

67123.539

Question#:	2
Topic:	financing
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Has the Department considered the use of third-party project financing for major capital investments that are likely to save money in the long run but face funding shortfalls now due to insufficient discretionary funding? Is this something that the Department is exploring for the St. Elizabeths headquarters project or for other major capital investment projects?

Does the Department require any additional authorities in order to use third-party project financing for St. Elizabeths or for other major capital investments?

Response: Yes, during the early planning stages for the DHS Consolidated Headquarters development at St. Elizabeths in 2006, the Department evaluated other financing mechanisms to phased direct appropriations. Third-party financing of the St. Elizabeths project by DHS would have to be done under enhanced use leasing authority similar to that granted to DOD in 10 U.S.C. 2667 § 2667. In accordance with the criteria in OMB Circular A-11, if enhanced used lease authority was utilized for a project such as St. Elizabeths, which would involve outleasing Federal land, development by a private entity, and leaseback of the resulting private structure, the resulting agreement would be a capital lease(s). In accordance with scoring rules, the net present value of the total cost of the capital lease would be scored as budget authority in the year budget authority was first made available for the lease. This would negate any budgetary benefit and result in larger costs to the taxpayer.

For the reasons stated above, third-party financing, under enhanced use leasing, would not be a viable alternative for financing the development of St. Elizabeths.

67123.540

Question#:	3
Topic:	risk management
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Government Accountability Office report notes that DHS has made important progress in analyzing risk across sectors but also highlights the need for DHS to use risk management more effectively to allocate its scarce resources. This is especially true now that the Department is in a very challenging budget situation.

GAO notes in its report that DHS needs to strengthen how it uses risk information to inform planning and budgeting. What is the Department doing to improve its use of risk information to support these processes?

Response: Given its large and diverse mission, the Department of Homeland Security (DHS) must allocate its limited resources across a wide array of missions, functions, programs and activities to maximize the safety and security of the nation. Risk, and the potential for its reduction, can provide one perspective through which DHS programs and activities can be meaningfully compared to help inform resource allocation decisions. As outlined in the Secretary's May 27, 2010 policy statement instituting Integrated Risk Management (IRM) across DHS, "The Department's adoption of IRM as a fundamental concept will guide its efforts within and across the homeland security enterprise. The goal of this policy is for DHS to use IRM to inform strategies, processes, and decisions to enhance security and to work in a unified manner to manage risks to the Nation's homeland security."

More specifically, the policy calls for:

> Develop[ment of] methodologies, where appropriate to determine the extent to which [the Department's] programs and activities manage and reduce risk to the Nation. DHS will use this information, among other inputs, to measure the Department's progress toward achieving strategic goals, inform decision-making, build its budget, help guide the allocation of limited resources, and promote understanding and collaboration among homeland security enterprise partners.

This mandate establishes the core requirement for a risk assessment to support the Planning, Programming, Budgeting and Execution (PPBE) process across the Department. It further identifies budget development and resource allocation as central applications of risk analysis for DHS. One example of a model that uses risk to support planning and budgeting decisions is the Risk Assessment Process for Informed Decision-making (RAPID).

67123.541

Question#:	3
Topic:	risk management
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

The goal of RAPID is to provide information about homeland security risks and the extent to which DHS programs and activities contribute to risk reduction to support DHS leadership decision-making during the annual PPBE cycle and supporting processes. To meet this goal, the objectives of RAPID are to:

- Produce a comparison of homeland security risks within and across incident types to support prioritization of efforts across the DHS portfolio;
- Map DHS programs and/or activities to homeland security risks and risk management areas for the purpose of understanding organizational alignment and identifying interdependencies and gaps among DHS actions;
- Assess programs and/or activities via comparable metrics of risk reduction to characterize disparate parts of the homeland security portfolio in terms of risk reduced and to allow for evaluation of potential enhancements and decrements in terms of risk reduction;
- Gather, aggregate, and analyze a wide range of risk data and information so as to support the ability to execute tailored analysis to address specific planning and programming questions within the PPBE process;
- Serve as a steward of data to support component-level and other risk analyses.

Following the execution of RAPID in 2010, DHS conducted a formal lessons learned process to prioritize improvements to future iterations of the assessment. The Office of Risk Management and Analysis also sponsored an independent review of the RAPID model conducted by a blue-ribbon panel of experts in risk and decision analysis. This process led to a formal confirmation of strategic requirements and reinforced the focus for RAPID in 2011-2012 on better understanding customer needs and the decision environment. Initial RAPID 2010 analysis provides a baseline view of homeland security risk and risk reduction across the Department's mission-oriented programs, portfolios, and/or activities.

67123.542

Question#:	4
Topic:	costs
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Future Years Homeland Security Program (FYHSP) report for Fiscal Years 2012-2016 includes data that indicate that management and administrative costs for the Department's seven major operational components (CBP, Coast Guard, FEMA, ICE, Secret Service, TSA, USCIS) are expected total $6.513 billion in FY 2012.

What is the Department doing to identify redundancies and inefficiencies within and across the management and administrative activities of its operating components, and to reduce or reallocate costs accordingly?

Response: Since the beginning of the Obama Administration, DHS has made an unprecedented commitment to efficiency in order to best support our frontline operations by building a culture of fiscal discipline and accountability.

Through the Department-wide Efficiency Review (ER) and other Department-wide initiatives, we have changed the way DHS does business, identifying over $3 billion in cost avoidances and cuts by streamlining operations and fostering a culture of greater transparency, accountability and fiscal discipline. To date, ER has launched 36 initiatives through which DHS has identified Department-wide cost avoidances as well as cost avoidances achieved through Component-specific initiatives.

Below are the DHS ER initiatives that have resulted in identification of cost avoidances for the Department.

- *Bulk Fuel:* DHS established an agreement with the Department of Defense to bulk purchase fuel at a lower rate – cutting its cost from $3.60/gallon to $2.97/gallon. DHS will achieve savings of $3 million annually beginning in FY 2012.

- *Encrypted Thumb Drives Blanket Purchase Agreement (BPA):* DHS plans to issue a strategically sourced contract vehicle for encrypted thumb drives in Fall 2012. DHS expects to achieve savings of $150,000 over a three-year period, beginning in FY 2013.

- *Energy Efficiencies/Energy Management:* In 2009 and 2010, DHS launched ER initiatives to reduce energy consumption and improve energy management. Through Component-led efforts to reduce energy consumption, such as installing energy efficient lighting and implementing power-management settings on

67123.543

Question#:	4
Topic:	costs
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

desktops and laptops, DHS has identified $3.9 million in cost avoidances since 2009.

- *Facilities Initiative:* Since 2009, DHS has identified more than $6.4 million in cost avoidances by using government office space and online tools for meetings and conferences instead of renting private facilities.

- *Fleet Management:* Through Component-led efforts to optimize fleet management through such efforts as "right-sizing" fleet inventory and transitioning to hybrid vehicles, DHS has identified more than $62 million in cost avoidances since 2009.

- *Furniture BPA:* DHS issued a strategically sourced contract vehicle for furniture in the National Capital Area in Fall 2011. DHS expects to achieve savings of $13.5million over a five-year period, beginning in FY 2012.

- *IT Inventory Management:* Since 2009, DHS has identified more than $16.8 million in cost avoidances through implementation of the Efficiency Review initiative to redeploy excess IT equipment inventory, such as servers and computers, throughout DHS instead of buying new equipment.

- *Multi-Functional Devices Initiative:* Since 2009, DHS has identified $4.8 million in cost avoidances through reducing expenditures on printers, copiers, and fax machines and procuring replacement multi-functional devices through a strategically sourced contract vehicle.

- *Non Military Uniforms BPA:* DHS plans to issue a strategically sourced contract vehicle for non-military uniforms in 2012. DHS expects to achieve savings of $6.9 million over a three-year period, beginning in FY 2013.

- *Office Supplies BPA:* Through use of the department-wide and the Federal government-wide strategically sourced contract vehicles for office supplies, DHS achieved a cost avoidance of $9.7 million since 2009.

- *Paperless ELS:* Since 2009, DHS has identified more than $2.3 million in cost avoidances through implementation of electronic paperless earning and leave statements across DHS and component-level efforts.

67123.544

Question#:	4
Topic:	costs
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

- *Personal Wireless Communication Devices/Services Optimization:* In 2010, DHS issued an Efficiency Review initiative that requires Components to conduct an annual optimization and validation of personal wireless communication services and devices to ensure DHS is not paying for services or devices that are not in use. Since 2009, DHS Components have avoided costs of $10.6 million by disconnecting wireless devices that were no longer being used and improving management of wireless communication services.

- *Printing Initiative:* Since 2009, DHS has identified more than $3.4 million in cost avoidances by minimizing printing and distribution of reports and documents that can be sent electronically or posted online.

- *Software Licenses Initiative:* In Fall 2011, DHS leveraged the purchasing power of the entire Department to acquire software licenses for Department-wide usage. DHS expects to achieve $180 million in cost avoidances over a seven year period.

- *Subscriptions Initiative:* Since 2009, DHS expects to avoid costs of $7 million in by consolidating subscriptions for Congressional Quarterly, LexisNexis, West Government Services, and Dun and Bradstreet and negotiating lower contract fees.

- *Tactical Communications BPA:* DHS plans to issue a strategically sourced contract vehicle for tactical communications equipment and services in 2012. DHS expects to achieve savings of $90 million over a five-year period, beginning in FY 2012.

- *Travel Initiative:* Since 2009, DHS has implemented efforts to eliminate non-mission critical travel and to maximize use of conference calls and web-based training and meetings, resulting in more than $13 million in cost avoidances. Through the continued use of web-based technology and communications, DHS expects travel cost avoidances to be realized annually. Under this Administration, DHS has reduced business class travel spending by nearly 90 percent.

- *Web-Based Notifications:* On June 1, 2011, DHS began implementation of an initiative submitted by a U.S. Customs and Border Protection employee that was selected as one of four finalists for the President's 2010 SAVE Award. The initiative changes current DHS practices by posting notices of seized property

67123.545

Question#:	4
Topic:	costs
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

online instead of in print newspapers. This initiative is expected to save approximately $1 million annually.

- *Wireless Communications Devices and Services BPA:* DHS plans to issue a strategically sourced contract vehicle for wireless communication devices and services in 2012. DHS expects to achieve savings of $36 million over a five-year period for, beginning in FY 2013.

- *Workforce Assessment Initiative:* Since 2010, DHS Components have identified more than $117 million in cost avoidances through contractor conversions. To further advance the appropriate balance between federal employees and contract services, the Department's FY 2012 budget proposed the conversion of 1,725 contract positions for an anticipated savings of $64 million.

DHS Components have implemented several efficiency initiatives at the operational level to reduce costs, improve processes, and achieve cost avoidances.

- *Contract Management:* Since 2009, DHS Components have identified more than $13 million in cost avoidances through improved contract management. DHS Components have implemented such efforts as restructuring contracts and utilizing DHS resources, rather than contractors, to perform mission-support activities to reduce costs.

- *Mission-Specific Initiatives:* DHS Components have identified more than $18 million in cost avoidances since 2009 by improving mission-critical processes.

- *Non-IT Equipment Management:* DHS Components have identified more than $1 million in cost avoidances since 2009 by re-utilizing excess equipment and improving management of excess equipment.

- *Process Improvement:* Since 2009, DHS Components have identified more than $15 million in cost avoidances by streamlining mission-support processes.

- *Property Management:* DHS Components have identified more than $10.9 million in cost avoidances by consolidating offices and purchasing, rather than renting, office space. "Purchasing office space" refers to a cost avoidance reported by Components. For instance, the Transportation Security Administration (TSA) purchased, instead of continuing to rent, the building for

67123.546

Question#:	4
Topic:	costs
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

the Transportation Systems Integration Facility, which evaluates airport security technologies prior to their development and acquisition, enabling TSA to improve system integration and field operating procedures.

- *Training:* Since 2009, DHS Components have identified more than $335 million in cost avoidances by developing trainings in-house and converting instructor-led trainings to web-based delivery.

DHS has also implemented other initiatives designed to cut costs and improve operations by targeting priority areas. These initiatives are listed below.

- DHS has been successful in implementing the Office of Management and Budget (OMB) Improving Acquisition Initiative, as well as in reducing our use of professional services contracts.
  - DHS has addressed high risk contracting by significantly reducing noncompetitive contracts. In FY 2010, DHS achieved its highest competition rate ever, competing 86 percent of its contract awards, computed using the OFPP competition rate methodology in effect for FY 2010.
  - DHS has achieved significant reductions in baseline spending through OMB's Acquisition Savings initiative, having already achieved savings of $1.13 billion from October 2009 thru June 2011.
  - DHS FY 2012 budget includes $105 million in additional professional services contracts savings.
- DHS is reviewing poorly performing IT projects for termination as part of its effort to reform IT. Using the TechStat model, DHS terminated the modernization project of the National Flood Insurance Program (FEMA) IT system and services, which is expected to result in a cost avoidance of $23.8 million.
- DHS is strategically consolidating data centers to drive IT efficiencies. To date, five DHS data centers have been closed resulting in savings of $18.7 million.
- DHS expects to achieve cost avoidances through improved management of its Federal real estate. In its Cost Savings and Innovation Plan which was delivered to OMB in September 2010, DHS identified cost savings of $179 million for 2012. DHS expects to achieve the savings through reduced operating expenses ($47 million), disposals ($6 million) and cancellation of a 1.7 million sq ft space requirement ($126 million).

67123.547

Question#:	5
Topic:	BUR
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In July 2010 you testified at a Committee hearing on the results of the Quadrennial Homeland Security Review (QHSR) and the Bottom Up Review (BUR). The BUR report identified 44 initiatives and enhancements that would be areas of priority for the Department over the next four years.

In general, what progress has been made to implement the Quadrennial Homeland Security Review and the Bottom Up Review since the Committee's hearing in July 2010? What BUR initiatives and enhancements has the Department prioritized during that time period?

Response: The submission of the QHSR Report to Congress on Feb. 1, 2010 marked an important first step in a multi-step process to examine and address fundamental issues that concern homeland security. The QHSR serves as foundational, cornerstone strategic guidance for homeland security activities across the homeland security enterprise in order to enhance the security and resilience of our Nation. QHSR strategic guidance is implemented throughout the entire programming and budgeting process, the oversight of major acquisitions, and strategy and planning within the Department.

The QHSR describes the nation's homeland security interests, identifies the critical homeland security enterprise missions, and ultimately defines a strategic approach to those missions by laying out the principal goals, essential objectives, and key strategic outcomes necessary for that strategic approach to succeed.

A bottom-up review (BUR) of the Department of Homeland Security, was published in July, 2010, as an immediate follow-on and complement to the QHSR. The BUR included an assessment of the organizational alignment of the Department with the homeland security missions set forth in the QHSR, including the Department's organizational structure, management systems, procurement systems, and physical and technical infrastructure. The BUR also included a review and assessment of the effectiveness of the mechanisms of the Department for turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan within the Department.

The Department's FY 2012 budget request, submitted to Congress in February, 2011, began the process of implementing the QHSR and specific BUR initiatives and enhancements, and the corresponding FY 2012-2016 Future Years Homeland Security Program set forth the budget plan required to provide sufficient resources to successfully

67123.548

Question#:	5
Topic:	BUR
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

execute the Department's responsibilities across the full range of homeland security missions as described in the QHSR. Further, the Department's approach to performance management and its priority goals are now guided by the QHSR and BUR, as reflected in the FY 2010-2012 Annual Performance Report and Plan, which was published in February 2011. In addition, the Department's forthcoming FY 2012-2016 Strategic Plan is founded on the framework and methodological approach of the QHSR and reflects performance measures aligned against the mission areas of the QHSR.

As part of the Budget and Execution phases of Planning, Programming, Budgeting, and Execution process, the Program Review Board and Acquisition Review Board, decision forums for programming and acquisition led within the Department by the Management Directorate, analyzes the extent to which Component Resource Allocation Plans reflect the strategic guidance of the QHSR. As part of the major acquisition oversight process set forth in Management Directive 102, the Office of Policy reviews Mission Needs Statements (MNSs) and Operational Requirements Documents (ORDs) to ensure their alignment with the QHSR. Finally, the QHSR serves as the foundation for the development of mission-specific strategies and analyses within the Department.

The following table lists the high-priority BUR initiatives identified by DHS and component leadership through the FY12-16 resource allocation process.

BUR initiative priority ranking	QHSR Mission	BUR Initiative
1	Mission 1	Strengthen aviation security
2	Mission 1	Create an integrated departmental information-sharing architecture
3	Mission 4	Increase DHS predictive and forensic capabilities for cyber intrusions and cyber-attacks
4	Mission 3	Improve the detention and removal process
5	Mission 1	Promote safeguards for access to secure areas in critical facilities
6	Mission 4	Strengthen DHS ability to protect cyber networks
7	Mission 2	Prioritize immigration and customs investigations
8	Mission 4	Promote cybersecurity public awareness
9	Mission 5	Improve DHS's ability to lead in emergency management
10	Mission 5	Make individual and family preparedness and critical facility resilience inherent in community preparedness

67123.549

Question#:	5
Topic:	BUR
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

11	Mission 2	Expand joint operations and intelligence capabilities, including enhanced domain awareness
12	Mission 2	Enhance the security and resilience of global trade and travel systems
13	Mission 3	Improve DHS immigration service processes
14	Mission 3	Focus on fraud detection and national security vetting

Question: What steps has the Department taken to implement the following five initiatives or enhancements that were identified in the BUR (please provide a separate answer for each):

Expand joint operations and intelligence capabilities, including enhanced domain awareness

Response: Several initiatives are proceeding with respect to this initiative. With respect to expanding joint operations and intelligence capabilities, as described in the DHS FY12 Budget in Brief, in partnership with the Drug Enforcement Administration (DEA) and the Department of Defense (DOD), DHS achieved initial operational capability for the new Border Intelligence Fusion Section within the El Paso Intelligence Center. The Border Intelligence Fusion Section will develop and disseminate a comprehensive Southwest Border Common Intelligence picture, as well as real-time operational intelligence, to our law enforcement partners in the region – further streamlining and enhancing coordinated federal, state, local, and tribal operations along the border. With respect to enhanced domain awareness, the Department conducted two successive requirements planning activities on domain awareness which identified the key capabilities needed to achieve Air, Maritime and Land Domain Awareness, and how these separate activities contribute to Integrated Domain Awareness. The results of this effort are currently being adjudicated within the Department.

Question: Align DHS operational activities in order to achieve maximum effectiveness

Response: This BUR initiative was combined with the BUR initiative on increasing the focus and integration of DHS's operational cybersecurity and infrastructure resilience activities. Primary implementation of this initiative is focused on transitioning the National Protection and Programs Directorate to a discrete operational component Planning is underway with respect to this initiative.

67123.550

Question#:	5
Topic:	BUR
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Realign component regional configurations into a single DHS regional structure

Response: The Department continues to assess ways to achieve a single regional structure and this effort remains a work in progress.

Question: Improve cross-Departmental management, policy and functional integration

Response: The Department has several ongoing efforts associated with this initiative. These include:

(a) The Department is prototyping an integrated investment life cycle model to strengthen strategic direction, assessment of mission need, and harmonize cross-cutting capabilities. Strengthening strategic direction, assessment of mission needs, and cross-cutting capability development harmonization will be accomplished via two new leadership bodies focused on decisions relating to strategy and requirements, to more fully address investments early in their life cycle. Pilot efforts have begun in 2011 to streamline the acquisition process and create a universal, cross-Component approach to program initiation and requirements review.
(b) DHS has requested FY12 funding for many initiatives that will strengthen management integration including Balanced Workforce Strategy, Human Resources Information Technology, and Data Center Migration.
(c) The Department continues to implement HSPD-12 to provide a single secure identification credential for all of DHS. For example, Personal Identity Verification (PIV) Card capability has been fully implemented at the USCG.

Question: Strengthen coordination within DHS through cross-Departmental training and career paths

Response: The Department's Chief Human Capital Officer is working with DHS Components to strengthen leader development Department-wide through the implementation of an integrated, coherent Leader Development Program, to include: 1) requirements and expectations for development at five leader levels; 2) Department-level processes for governance, policy, and investment strategies; and 3) corporate succession programs to build a continuous pipeline of leadership talent from emerging to executive leaders.

The Leader Development Initiative will deliver competency-based leader training to support executives, managers, and supervisors at all levels of leadership within the Department. The Workforce Training program will implement a comprehensive framework for identifying critical skill gaps and competencies for mission critical occupations and performing related competency assessments Department-wide.

67123.551

Question#:	6
Topic:	PAE
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Section 702(b)(2) of the Homeland Security Act requires that the Office of Program Analysis and Evaluation (PA&E) in the Department "provide leadership in developing and producing improved analytical tools and methods for analyzing homeland security planning and the allocation of resources."

How would you assess the adequacy of existing analytical tools and methods for analyzing homeland security planning and the allocation of resources?

What steps has PA&E taken to improve these tools and methods in the last several years?

Response: DHS has made significant progress in developing appropriate analytic tools and methods supporting DHS planning and resource allocation. However, our methods and tools are continuing to improve and mature. Areas where we are seeking to make improvement include our understanding of costs and the long range implications of investment, as well as use of modeling to evaluate performance achieved by alternative capital asset profiles or to project force structure. Particularly in a constrained fiscal environment, it is imperative that these analytic capabilities be instituted so that DHS can optimize mission outcomes through effective and efficient resource allocation.

Program Analysis and Evaluation (PA&E) has taken numerous steps in recent years to improve our tools and methods. For example:

- The Bottom-Up Review (BUR) was a DHS-wide effort that resulted in a new suite of programs and activities that the Department uses to inform internal resource allocation decision making with greater comparability across the organization. The review set the groundwork for proposing standardized appropriation account structures that will provide greater visibility into how resources are applied to support the DHS missions articulated in the Quadrennial Homeland Security Review.
- PA&E worked with OCIO to improve our Future Years Homeland Security Program information technology system restructured with a module to accommodate the resource data resulting from the BUR effort and make it available to other DHS organizations to reuse program and budget information for acquisition oversight and capital planning. This Program Data Module (PDM) is an interactive repository into which components enter planning data by the program, activity and account structures. These data are mapped to the DHS

67123.552

Question#:	6
Topic:	PAE
Hearing:	Defending the Nation since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

mission framework and to performance data enabling a more structured approach to analysis and decision making.

  - Examples of processes and decision support tools informed by the PDM include: the annual budget and resource review process, the Integrated Investment Lifecycle Cost Model pilots, Capital Asset Plan and Business Case Summaries (exhibits 300), information technology portfolio reviews and various internal reports and analyses.

- PA&E is working to better integrate capital investments plans into the PDM to provide a single source of data entry and access supporting the processes and tools described above. As such, the PDM will become a single repository of funding information supporting multiple users and decision support tools.
- PA&E continues to conduct independent program evaluations and studies primarily through the Homeland Security Studies and Analysis Institute (HSSAI) but also with other organizations. The office is also improving the organic capability of internal staff to conduct these evaluations. A DHS Cutter Study completed in July of 2011 is an example of staff led independent, objective evaluation informing resource allocation decision-making by leadership presented with alternatives analysis and empirical data regarding the performance of trade-offs in investment.

Building on these accomplishments, PA&E continues to mature staff, tools and methods to better inform optimal allocation and use of scarce homeland security resources.

67123.553

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Ten Years After 9/11: Are We Safer?
Chairman Joe Lieberman
September 13, 2011

Good morning, the hearing will come to order. I want to welcome our distinguished panel of witnesses, Secretary Napolitano, Director Mueller and Director Olsen, testifying for the first time since his confirmation.

This past weekend, in ceremonies and vigils across the nation, we stopped to remember the nearly 3,000 people who were killed ten years ago in the attacks of September 11, 2001 and to appreciate the acts of heroism and service by countless Americans on that day and every day since to protect our homeland and defeat the violent Islamist extremists who attacked us on 9/11.

The 9th anniversary of 9/11 last year didn't get the same degree of attention. And neither will the 11th anniversary next year. And in some sense that's why we're here this morning. This annual hearing on the status of the threat against our homeland with the heads of these three critically important agencies has become a tradition. And Senator Collins and I very much wanted to hold it after 9/11 to look back a little bit, but really to look forward and make the point that our work goes on.

Even though we had fresh warnings that alerted us over the past few days, there's already evidence that, in a quite natural reaction, Americans are beginning to forget how real the threat of violent Islamist extremism continues to be. There was a Gallup poll taken last year that showed terrorism ranked at the bottom of six concerns that people had -- probably because of the intensity of economic problems – behind the economy, jobs, government corruption, federal spending, and health care. And just last week a study published by the Cato Institute called for abolishing the Department of Homeland Security – which essentially would return us to where we were pre 9/11.

In some ways we may be the victims of our own success in protecting the homeland since there has not been another mass-casualty terrorist attack on American soil since 9/11 – a reality that, ten years ago, no one would have dared to predict.

Some have taken this lack of another large-scale attack as further evidence that the U.S. government exaggerated the danger posed by Islamist extremism and "overreacted" in the wake of 9/11.

I believe this is a profoundly mistaken and ultimately irresponsible conclusion. We have weakened our enemies and protected our homeland but our enemies are not vanquished. That's why our vigilance must be constant and not limited to the attention for a particular anniversary.

As the Senate Committee on Homeland Security, it's our responsibility to make sure the national focus is not distracted from the threat. For our witnesses and the tens of thousands of people who work with them, it is

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.554

their constant responsibility to protect our homeland. So we welcome them to this annual threat hearing and thank them for the service and for all that their respective agencies have done to ensure that we have not had another terrorist attack in the next ten years.

But the violent Islamist extremism ideology that inspired the attacks of 9/11 remains a potent force, though weakened throughout the world, and has had an effect in the radicalization of homegrown terrorists. Today we've asked our three witnesses to help us answer at least three big questions.

One is to take a look back at what the U.S. government and their agencies have done since 9/11. Two, the focus of this hearing is to discuss the status of the current threat of Islamist terrorism to our homeland. The third is to discuss what our government currently is doing to counter that threat.

So for me, the question today is not 'are we safer than we were on 9/11?' I think it's self-evidently clear that we are safer. The question is 'what are we doing and what should we be doing to ensure that safety continues to be what it is and is strengthened in the face of the challenges we face?'

The ten year anniversary of 9/11 has passed, the media and public attention will naturally fade, but this congress and future congresses, and this administration and future administrations, must stay focused on the threat and its ever-evolving tactics until the ideology is truly vanquished and gone.

67123.555

Opening Statement of
Ranking Member Senator Susan M. Collins

"Ten Years After 9/11: Are We Safer?"

Committee on Homeland Security and Governmental Affairs
September 13, 2011

The State of Maine became forever linked to the attacks of September 11th, 2001, when two of the hijackers, Mohammed Atta and Abdulaziz al Omari boarded an early morning flight to Boston at the Portland Jetport. From Logan Airport, they set in motion the worst terrorist attack in our nation's history by seizing control of American Airlines Flight 11.

That evening, Members of Congress came together on the steps of the Capitol to express unity. A day that began with shock and anger ended with unity and resolve.

We resolved to ensure our country had the tools to deter and detect future plots and to identify those who would do us harm. When Chairman Lieberman and I authored the Intelligence Reform and Terrorism Prevention Act of 2004, our goal was to create a strong leader to coordinate the 17 separate agencies of the Intelligence Community and to change their culture from "need to know" to "need to share" so that next time the dots would be connected in time to stop an attack.

The operation that killed Osama bin Laden represented the kind of successful collaboration of intelligence and operations that we envisioned. Information is now being shared more effectively, both across the federal government and among federal agencies and their state, local, and tribal partners.

Just last week, DHS and the FBI announced a "specific, credible but unconfirmed threat" related to the 9/11 anniversary. The Administration is took this threat seriously and shared intelligence with state and local enforcement officials in the targeted locations and with others across the country.

Thankfully, there was not an incident over the weekend. But we must consider whether this particular threat has truly passed and for how long we should remain on heightened alert.

This threat demonstrates yet again that the terrorists have not abandoned their quest to harm our country and continue to probe for vulnerabilities.

67123.556

Much has changed in the past decade. We have vastly improved the sharing of information across agencies at the federal level and with state and local emergency and law enforcement professionals.

Joint Terrorism Task Forces are now based in 106 cities nationwide. JTTF personnel come from more than 600 state and local agencies and 50 federal agencies.

State-based fusion centers have established a two-way street with our federal partners and our first responders, who are likely to be the first to observed suspicious activity.

In the case of last week's terrorist threat, the decision to publicize the threat put millions of eyes and ears on the lookout for suspicious behavior on the eve of the September 11th commemoration.

Senator Lieberman and I continue to work to expand the "See Something, Say Something" law. Our bill would provide further protection against lawsuits for citizens who report suspicious behavior indicating potential terrorist activity.

When it comes to our homeland security, we are, however, only as strong as our weakest link. As we saw in 2009, with the Christmas Day bomber and Major Hasan's attack on Fort Hood, when information is not shared and when warning signals are ignored or overlooked, our security is placed at risk.

The TSA has strengthened airline passenger screening. Nevertheless, a young man was recently able to fly cross-country without a valid ID and with an expired boarding pass that was not even in his name.

Similarly, the Department of Homeland Security has bolstered the security of U.S. borders and identification documents, yet two Iraqi refugees with ties to al Qaeda were arrested in Kentucky for allegedly helping to carry out attacks against our troops.

How a known bomb maker, whose fingerprints we had had for years, was able to enter our country on humanitarian grounds remains an unanswered and troubling question. It appears, however, that this case may reflect the lack of imagination that the 9/11 Commission found to be a persistent failure. While the FBI's analysis of IEDs collected in Iraq and Afghanistan has undoubtedly helped U.S. warfighters, the forensic information being collected from these devices should also be used to screen those seeking to enter our country.

We must ask: Are there other Iraqi nationals granted asylum who were involved in attacking our troops? I know the Administration is reviewing the

67123.557

files of the more than 51,000 Iraqi's admitted under this refugee program, but it is deeply troubling that we still await clear answers from the Administration.

Homegrown terrorism is another evolving threat that continues to challenge us. This Committee first sounded the alarm about home-based terrorism five years ago and has held more than a dozen hearings on the topic.

Over the past two years, 31 arrests were made in "homegrown" plots by American citizens or legal permanent residents, an enormous increase compared to the previous seven years dating back to 2001. Yet, the Administration's strategy for countering violent Islamist extremism is insufficient to meet the threat.

We shall never forget those we lost on September 11th, 2001. As has been noted often, the terrorists only have to get it right once; we have to be right every time or suffer the consequences of an attack. We are much safer than we were a decade ago, but we must be relentless in anticipating the changing tactics of terrorists. As the successful decade-long search for Osama bin Laden proved, America's resolve is the most powerful weapon against those who seek to destroy our way of life.

67123.558

Opening Statement of Senator Jerry Moran of Kansas

Committee on Homeland Security and Government Affairs
Ten Years after 9/11: Are We Safer?

September 13, 2011

Chairman Lieberman and Ranking Member Collins, thank you for holding this hearing today. Mr. Chairman, our government's primary responsibility is the protection of its citizens. No one will ever forget that September morning 10 years ago when they heard the news that America was under attack. In a matter of minutes, lives were forever changed as fire fighters rushed to answer the cries for help, citizens risked their lives to save others, and final phone calls were made to loved ones. As President Bush said this weekend at the National Memorial dedication for Flight 93 in Pennsylvania, that day taught us that "evil is real, and so is courage."

After the attacks on September 11th, I traveled to New York to witness the destruction at Ground Zero firsthand. Around the smoldering pile of rubble was a makeshift memorial where flowers, photos, and prayers in tribute to the fallen had been left. One note caught my eye; it was penned on spiral notebook paper. It read: "Dear Daddy – How much I miss you. I hope heaven is a wonderful place. I hope I live a life good enough to join you there someday – Amanda, age 12." One of my own daughters was 12 at the time, so Amanda's words left a lasting impression on me. At that moment, I resolved to work toward the day when there would never again be notes left behind by children like Amanda.

Today we are closer to achieving that goal, but there is still work to be done. Secretary Napolitano, Director Mueller, and Director Olsen, I look forward to hearing your testimony on the progress we've made and the work ahead to ensure we live up to our most important responsibility. It is our duty to preserve this nation for the next generation – so they too can pursue the American dream. Thank you Mr. Chairman.

67123.559

Testimony of

Secretary Janet Napolitano

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Government Affairs

September 13, 2011

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00934 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.560

Introduction

Thank you, Chairman Lieberman, Senator Collins, and members of the Committee. I appreciate the opportunity to testify today on the Department of Homeland Security's efforts to keep our nation safe from evolving threats.

The United States has made significant progress in securing the nation from terrorism since the September 11, 2001 attacks. As we observe this tenth anniversary of 9/11, we honor the nearly 3,000 innocent victims, as well as their friends, colleagues, and families. We salute the many first responders and law enforcement officials who responded with such courage and conviction on that tragic day and in the days that followed.

We also recommit ourselves to the continued protection of our nation, our freedoms, and our way of life. The recent anniversary is also a time to consider the great progress we have made since then. America is a stronger and more secure nation today. We bounced back from the worst attack on our soil and made progress on every front to protect ourselves, using our experience to become more resilient, not only to terrorist attacks, but to threats and disasters of all kinds.

Following 9/11, the federal government, including many members on this committee, such as Senators Lieberman and Collins, moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, and local capabilities to prepare for, respond to, and recover from attacks and disasters at home.

A key element of this new security framework included the creation of the Department of Homeland Security (DHS) in March, 2003, bringing together 22 separate agencies and offices into a single, Cabinet-level department. Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners across the federal government, public and private sectors, and communities throughout the country have strengthened the homeland security enterprise to better mitigate and defend against dynamic threats.

Additionally, within the federal government, many departments and agencies contribute to this homeland security mission. The nation's armed forces serve on the front lines of homeland security by degrading al-Qa'ida's capabilities to attack the United States and targets throughout the world. The Office of the Director of National Intelligence, the Central Intelligence Agency, and the entire Intelligence Community, of which DHS is a member, are producing better streams of intelligence than at any time in history.

The federal homeland security enterprise also includes the strong presence of the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), whose role in leading terrorism investigations has led to the arrest of more than two-dozen Americans on terrorism-related charges since 2009.

We have also worked to build and strengthen the homeland security enterprise far beyond DHS and the federal government. A key part of the enterprise includes working directly with law

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00935 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.561

enforcement, state and local leaders, community-based organizations, and private sector partners to counter violent extremism at its source, using many of the same techniques and strategies that have proven successful for decades in combating violent crime in American communities.

Today I would like to highlight some of the Department's most significant work to address specific recommendations from the 9/11 Commission Report in the following areas:

- Expanding Information Sharing
- Developing and Implementing Risk-based Transportation Security Strategies
- Strengthening Airline Passenger Pre-screening and Targeting Terrorist Travel
- Enhancing Screening for Explosives
- Strengthening Efforts to Detect and Report Chemical, Biological, Radiological and Nuclear Threats
- Protecting Cyber Networks and Critical Physical Infrastructure
- Bolstering the Security of U.S. Borders and Identification Documents
- Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

While challenges remain, DHS continues to focus on minimizing risks while maximizing the ability to respond and recover from attacks and disasters of all kinds. This is a challenge that the more than 240,000 men and women of DHS commit themselves to everyday, with the support of Congress, our many partners within and outside of government, and the American people.

A 9/11 Timeline and Security Enhancements

Perhaps the best way to illustrate the concrete progress made over the past ten years is to apply today's security architecture to what existed when the terrorist attacks of 9/11 occurred.

The 9/11 plot, like many terrorist plots, began overseas, which means our security layers must start there as well.

- Intelligence: Planning for 9/11 began several years before the actual attacks. Osama Bin Laden summoned operatives to Afghanistan to discuss using commercial aircraft as weapons. Since then, we have strengthened the depth and breadth of our intelligence enterprise to get the best information possible, wherever the operational planning may occur.

- Visa Security: All of the 9/11 hijackers applied for visas overseas. Today, the DHS Visa Security Program deploys trained special agents to high risk posts around the world to conduct targeted, in-depth reviews of visa applicants before they ever reach the United States. We have additional layers of security in place through Department of State (DOS) visa checks and pre-departure screening measures.

- International Information Sharing: The hijackers began preparing for the attack while living abroad. Today 18 countries have joined the United States in agreeing to share information about potential terrorists and criminals through a series of Preventing and Combating Serious Crime Agreements. This is in addition to the many international

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00936 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.562

Mutual Legal Assistance Treaties and other arrangements with our partners and others in the international community.

After 9/11, the federal government discovered that information existed about the hijackers well before and after they came to the United States but this information had not been coordinated, shared and analyzed. Since 9/11, the federal government, along with its state, local, and private sector partners, has made significant improvements to enhance information sharing and analysis.

- Targeting: The federal government, and DHS in particular, has become more effective at analyzing travel-related data to better understand and anticipate the travel patterns of known or suspected terrorists. This analysis has been essential in identifying, targeting, and interdicting known and suspected terrorists – and prompting additional screening – before these individuals travel to the United States.

- Fusion Centers: Today, 72 recognized fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information among the federal government and state, local, tribal, territorial and private sector partners. Today the Intelligence Community is able to identify the common threads that can tie a seemingly minor crime to the larger threat picture – an important step that helps us to identify individuals such as the hijackers, many of whom were apprehended by law enforcement for routine traffic violations prior to 9/11.

Once the 9/11 hijackers made it to the United States, they still required access to the aircraft.

- Flight School: Prior to 9/11, the hijackers enrolled in flight school and conducted cross-country surveillance flights. Today, the Transportation Security Administration (TSA) screens all foreign students seeking flight training against terrorist, criminal history and immigration databases.

- Passenger Screening: Ten years ago, the 9/11 hijackers were able to purchase tickets and board planes carrying weapons. Today, through the Secure Flight program, DHS prescreens 100 percent of the 14 million passengers flying weekly to, from, and within the United States against the government watch lists. This enables us to identify and prevent individuals on the No Fly List from boarding aircraft and recommend others for enhanced screening. Moreover, Transportation Security Officers at more than 450 airports screen all checked and carry-on baggage for explosives, weapons, and other threats using cutting-edge technologies.

- Behavior Detection: Even though some of the 9/11 hijackers were randomly selected for additional screening and aroused the suspicion of gate agents, they still made it onto the plane. TSA's Behavior Detection Officers today work to identify potentially high-risk passengers who exhibit behaviors that indicate they may be a threat to aviation security and refer them for additional screening. TSA also conducts screening of passengers at boarding gates based on intelligence to help our security officers focus appropriate resources on determining if an individual presents a higher risk. Behavior Detection

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00937 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.563

serves as an important additional layer to enhance security in the airport environment, and can easily be deployed to other modes of transportation.

The last line of defense against threats to aviation security is on the plane itself.

- Airplane Security: Today, all commercial aircraft have hardened cockpit doors and Federal Air Marshals are deployed across the aviation system based on risk. Additionally, the Federal Flight Deck Officer program allows qualified pilots to use firearms to defend the cockpit, and TSA runs a crewmember behavior recognition and response training program. Taken together, these efforts significantly enhance the safety and security of passengers on board.

- Emergency Communications: Limitations in communication and interoperability among air traffic control operators, military personnel and first responders hindered the response on 9/11. Our nation has since made significant investments in training and technical assistance to improve emergency communications capabilities.

All of these layers combined create a much stronger security architecture that did not exist on 9/11 and that has helped keep our nation, our transportation system, and the American people safe over the past ten years.

During this time, we have also worked hard to create a unified and integrated department, focusing on accountability, transparency and leadership development, to enhance mission performance. This effort includes an ambitious series of management integration reforms to ensure the Department has the proper management structures and acquisition strategies necessary to succeed, attract and retain top talent, and build a culture of efficiency.

Progress Addressing Key Recommendations of the 9/11 Commission

Expanding Information Sharing

Over the past several years, DHS has strengthened and evolved our homeland security enterprise to better mitigate and defend against dynamic threats. This approach is based on the simple premise that homeland security begins with hometown security. Through close partnerships with federal, state, tribal, and local governments, community-based organizations, and private sector partners, DHS works to ensure that resources and information are available to state and local law enforcement, giving those on the frontlines the tools they need to protect local communities.

As part of this approach, we have supported the creation of 72 state and local fusion centers across our country, where information about threats is gathered, analyzed, and shared among our partners. Fusion centers also support and regularly interact with FBI Joint Terrorism Task Forces, which coordinate resources and expertise from across the federal government to investigate terrorism cases.

Since 9/11, DHS and DOJ have worked to establish and strengthen the Nationwide Suspicious Activity Reporting Initiative, which for the first time trains law enforcement across our country

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00938 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.564

to recognize behaviors and indicators related to terrorism and crime, and standardizes how those observations are documented, analyzed, and shared.

To help counter the threat of violent extremism in our communities, DHS also has trained more than 46,000 front-line law enforcement professionals, and worked with hundreds of communities and local organizations, to implement community-oriented policing strategies that have proven successful in crime-reduction efforts in some of our biggest cities.

In addition, we have implemented a new National Terrorism Advisory System (NTAS), which provides timely, detailed information about terrorist threats and recommended security measures to the public, government agencies, first responders, transportation hubs, and the private sector. Under NTAS, DHS coordinates with other federal entities to issue detailed alerts to the public when the federal government receives information about a specific, credible terrorist threat to the United States.

We also have worked to engage the broadest set of partners possible in our security efforts, because the reality is that no government entity, by itself, can protect a nation of our size and diversity. To this end, we have continued to strengthen and expand the "If You See Something, Say Something™" campaign, a nationwide effort to increase public awareness and the reporting of suspicious aetivity to the authorities. This campaign began in New York City, with the Metropolitan Transportation Authority of the State of New York. We have since expanded it to transit systems, federal buildings, major sports and entertainment venues, and major U.S. retailers.

In collaboration with the "If You See Something, Say Something™" campaign, TSA is also providing, through its First Observer™ program, training for thousands of state and local law enforcement personnel and private sector employees on how best to observe, assess, and report suspicious behavior at transportation and critical infrastructure sites and facilities across the country.

We also have focused on building stronger relationships with our many partners, including federal agencies, tribal governments and law enforcement, the private sector, and our international partners.

DHS works closely with its partners across the federal government on various information sharing initiatives to support law enforcement operations and protect the country from terrorists and other threats. For example, DHS has provided hundreds of personnel to FBI JTTFs, including U.S. Immigration and Custom Enforcement (ICE) special agents, U.S. Secret Service (USSS) agents, Federal Air Marshals, U.S. Customs and Border Protection (CBP) officers, U.S. Citizenship and Immigration Services (USCIS) officers and representatives from the Federal Emergency Management Agency (FEMA) and the U.S. Coast Guard (USCG).

DHS also has expanded our work with tribal governments and law enforcement across the nation. In 2009, DHS designated tribal liaisons in every operational component to work directly with tribal communities, and in 2011, DHS announced a new DHS Tribal Consultation Policy

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00939 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.565

outlining the guiding principles under which all elements of the Department are to engage with sovereign tribal governments.

The private sector also remains an integral component of the homeland security enterprise, and through the Department's Private Sector Office, we have worked to improve coordination of private sector engagement across the Department, facilitating more effective and rapid communication with key organizations and bolstering regionally-focused information sharing efforts.

Developing and Implementing Risk-based Transportation Security Strategies

DHS focuses on risk-based, intelligence-driven security across all modes of transportation. This approach emphasizes pre-screening for passengers and cargo to expedite travel for individuals that law enforcement knows the most about, while focusing limited resources on those who pose the greatest threat to the nation's transportation networks.

We have made significant advances in risk-based security, including conducting baseline security assessments across aviation, maritime, and surface transportation sectors; historic global aviation standards; advanced passenger and cargo information; and enhanced information sharing with international and private sector partners.

For example, after the attempted terrorist attack against Northwest Airlines Flight #253 on December 25, 2009, DHS launched an unprecedented initiative to strengthen global aviation against threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry. These efforts culminated at the International Civil Aviation Organization (ICAO) Triennial Assembly in October 2010, where nearly 190 countries of the Assembly adopted the Declaration on Aviation Security, which forges a historic new foundation for aviation security to better protect the entire global aviation system and make air travel safer and more secure than ever before.

In June 2010, TSA also provided to Congress the Transportation Sector Security Risk Assessment report, a nationwide risk assessment that examines the potential threats, vulnerabilities, and consequences of a terrorist attack involving the nation's transportation system, including the aviation and surface domains. This report has informed the development of risk mitigation strategies, security standards, countermeasures, and resource allocations.

Since 2006, TSA also has completed more than 190 Baseline Assessments for Security Enhancement for mass transit, which provides a comprehensive assessment of security programs in critical transit systems around the country. Additionally, the DHS Science and Technology Directorate (S&T) has conducted detailed vulnerability analyses for all U.S. underwater mass transit tunnels. Since 2006, DHS has awarded over $2 billion in Surface Transportation Security Grants to help protect the public and nation's critical transportation infrastructure against acts of terrorism and other large-scale events.

DHS is also focused on strengthening maritime transportation security through a risk- and technology-based approach by evaluating vulnerabilities and mitigating threats across all

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00940 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.566

potential pathways. To this end, the United States Coast Guard's mix of cutters, aircraft, and boats as well as their unique authorities enhance layered maritime security from inspections at foreign ports of departure to patrols at the critical ports within our homeland. These measures increase transparency of activity, reduce risk, and maximize the effectiveness of maritime security resources.

To support state and local efforts to strengthen maritime security, since fiscal year 2003, DHS has provided more than $2 billion in grants for the Port Security Grant Program (PSGP) – awarded based on risk – to protect critical port infrastructure from terrorism, enhance maritime domain awareness and risk management capabilities, and support the implementation of the Transportation Worker Identification Credential (TWIC).

Enhancing Global Supply Chain Security

Immediately following the thwarted terrorist plot to conceal and ship explosive devices on aircraft bound for the United States in October 2010, DHS also worked with industry to implement additional precautionary security measures for international inbound flights. Today, DHS continues to work with leaders from global shipping companies and groups such as the International Air Transport Association (IATA) on developing preventive measures, including terrorism awareness training for employees and vetting personnel with access to cargo.

DHS is also working with agencies throughout the Administration to develop a unified vision for global supply chain security across air, land, and sea modes of transportation. The implementation of this strategy will more comprehensively address risk than ever before.

In support of our supply chain security efforts, CBP continues to operate the Container Security Initiative (CSI) to ensure that U.S.-bound maritime containers that pose a potential risk are identified and inspected before they are placed on vessels destined for the U.S. CSI, which was first announced in January 2002, is currently operational in 58 foreign seaports in 32 countries.

In January 2010, CBP also began enforcement of the Importer Security Filing and Additional Carrier Requirements interim final rule – also known as the "10 + 2 rule" – increasing the scope and accuracy of information gathered on cargo shipments arriving by sea into the United States and bolstering our layered enforcement strategy to protect against terrorism and other crimes at U.S. ports of entry. Further, CBP manages the Free and Secure Trade (FAST), a commercial clearance program for known low-risk shipments entering the U.S. from Canada and Mexico. Initiated after 9/11, FAST allows expedited processing for commercial carriers who have completed background checks and fulfill certain eligibility requirements.

In addition, the USCG's International Port Security personnel also inspect ports to ensure compliance with anti-terrorism protection measures and the International Ship and Port Facility Code. The USCG's International Training Team also works with the Department of State to build the capacity and proficiency of a foreign nation's Coast Guard and Naval forces to increase global supply chain security.

Strengthening Airline Passenger Pre-screening and Targeting Terrorist Travel

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00941 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.567

Prior to 9/11, screening of passengers coming to the United States was limited to the Department of State visa process and the inspection of a person by an immigration officer at the port of entry. Provision of advance passenger information (API) by airlines was voluntary and often inconsistent.

Over the past eight years, DHS has significantly adapted and enhanced its ability to detect threats, building a layered, risk-based system that includes a full range of identification verification measures – from visa application checks and biometric identification to the receipt of advanced passenger information and the full implementation of Secure Flight, a program that enables DHS to prescreen 100 percent of passengers flying to, from, or within the United States against government watchlists. DHS has also increased enrollment in its trusted traveler programs—which expedite travel for members who pass rigorous, recurrent security checks— to over one million members.

With support from international partners and the aviation industry, DHS has implemented pre-departure programs for U.S. bound flights as well as enhanced security measures to strengthen the safety and security of all passengers. These new measures, which cover 100 percent of passengers traveling by air to the United States, utilize real-time, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

DHS has worked closely with the intelligence and law enforcement communities to develop new mechanisms that identify high-risk travelers prior to departure. The U.S. Government has reformed the criteria and nomination processes for the consolidated terrorist watchlist and enhanced its information sharing capabilities to comprehensively connect available pieces of intelligence. This allows us to better identify individuals who are known to be of security concern as well as those individuals that would otherwise remain unknown.

Today, four centers across the federal government provide information regarding potential terrorist travel: Terrorist Screening Center (TSC), National Counterterrorism Center (NCTC), the National Targeting Center, and the Human Smuggling and Trafficking Center, all of which work together, leveraging threat-related intelligence and travel-related data which is essential in identifying, targeting, and interdicting known and suspected terrorists as well as suspicious cargo prior to entering the United States or boarding a flight bound for the United States.

In addition, information that previously had been retained at entry points in the United States is now shared overseas earlier in the travel continuum so that suspect travelers do not board an airplane departing for the United States without, at a minimum, additional screening. In fiscal year 2010, DHS identified more than 1,500 passengers on watchlists who had booked international flights departing to the United States. These passengers were denied boarding, received enhanced security screening, or were removed from the watchlist after it was determined that they did not pose a threat.

Prior to 9/11, there also was no advance screening of passengers seeking admission under the Visa Waiver Program (VWP), which enables nationals of 36 designated countries to travel to the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00942 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.568

United States as nonimmigrant visitors for stays of 90 days or less without obtaining a visa. In 2008, DHS implemented the Electronic System for Travel Authorization (ESTA) to screen prospective VWP travelers against several databases, including the terrorist watchlist; lost and stolen passports; visa revocations; previous VWP refusals; and public health records. Since January 2009, nationals from all 36 VWP countries, regardless of their port of embarkation, have been required to obtain an approved travel authorization via ESTA prior to boarding a carrier to travel by air or sea to the United States under the VWP.

DHS – in cooperation with Departments of State and Justice – also has made substantial progress in bringing VWP countries into compliance with the information sharing requirements of the 9/11 Act, which requires VWP countries to enter into an agreement with the United States to report, or make available to the United States, lost and stolen passport data so that it can be screened against INTERPOL's Stolen and Lost Travel Document database. This requirement has contributed to the overall decline of fraudulent VWP passport intercepts at the U.S. border, from 712 in Fiscal Year 2004 to 36 in Fiscal Year 2010.

In addition, VWP countries must enter into an agreement to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens. The Preventing and Combating Serious Crime Agreement, mentioned previously, goes toward satisfying this statutory requirement.

Through the Visa Security Program (VSP), with Department of State concurrence, ICE deploys trained special agents overseas to high-risk visa activity posts in order to identify potential terrorist and criminal threats before they reach the United States. ICE special agents conduct targeted, in-depth reviews of individual visa applications and applicants prior to visa issuance, and make recommendations to consular officers regarding refusal or revocation of visas when warranted. The VSP is currently deployed to 19 posts in 15 countries.

Advanced Passenger Information, Passenger Name Records, and Risk-Based Security

To identify high-risk travelers and facilitate legitimate travel, DHS requires airlines flying to the United States from foreign countries to provide Advanced Passenger Information (API), which includes basic information such as name, date of birth, citizenship/nationality and passport number, and Passenger Name Records (PNR), which includes information that travelers provide to airlines when booking their flights, such as itinerary, address, and check-in information, up to 72 hours prior to departure. Since the creation of the Department, DHS has improved its ability to use this and other information to target and identify both known and unknown individuals that are either a threat to aviation or the United States, and to prevent them from either flying to or entering the United States.

During 2008 and 2009, PNR helped the United States identify individuals with potential ties to terrorism in more than 3,000 cases, and in Fiscal Year 2010, approximately one quarter of those individuals denied entry to the United States for having ties to terrorism were initially identified through the analysis of PNR.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00943 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.569

DHS and the European Union (EU) are completing a new U.S.-EU PNR agreement that improves the privacy protection and security benefits of the 2007 U.S.-EU PNR Agreement currently in effect. The new PNR Agreement, which requires approval by the Council of the European Union and ratification by the European Parliament, will underscore the United States and the European Union's continuing commitment to combat terrorism and serious transnational crime, while respecting privacy.

As noted earlier, DHS also fully implemented Secure Flight in November 2010, fulfilling a key 9/11 Commission recommendation. Secure Flight uses the passenger's full name, date of birth, gender, and if applicable, redress number, to conduct watch list matching prior to issuing the passenger a boarding pass. In addition to facilitating secure travel for all passengers, this program helps prevent the misidentification of passengers who have names similar to individuals on terrorist watchlists. Prior to Secure Flight, airlines were responsible for checking passengers against the watchlists. Through Secure Flight, TSA now vets over 14 million passengers weekly. In addition, DHS currently has eight Immigration Advisory Program arrangements in six countries, which enable our CBP officers posted at foreign airports to use advanced targeting and passenger analysis information to identify high-risk travelers at foreign airports before they board U.S.-bound flights.

In order to facilitate legitimate travel and effectively deploy screening and security resources, CBP has increased enrollment in its Trusted Traveler programs from approximately 80,000 members in 2003 to over one million today. CBP currently manages three Trusted Traveler Programs for the passenger environment: NEXUS, the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Global Entry, and now offers a single, online trusted traveler application for all modes of travel. These programs expedite travel into the United States for pre-approved, low-risk members who voluntarily apply, pay a fee, provide biometric identification, pass a rigorous background check, and undergo recurrent security checks.

Recognizing that security screening must be constantly updated to address evolving threats, the Administration continues to focus on the implementation of risk-based measures to strengthen aviation security while improving the passenger experience wherever possible. TSA is currently working on a variety of identity-based screening measures that would enable travelers to volunteer more information about themselves, prior to flying, in order to expedite physical screening. This is an ongoing, collaborative effort with law enforcement, airport authorities, the aviation industry, and the traveling public. As risk-based screening evolves, DHS and TSA will continue to incorporate random security steps as well as other measures, both seen and unseen, in order to maintain the safest and most efficient system for the traveling public.

Enhancing Screening for Explosives

Prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today all checked and carry-on baggage aboard aircraft is screened for explosives. Increased levels of frontline security personnel at the passenger checkpoints and new technologies have also significantly enhanced security. In March 2002, TSA's first cadre of federal screeners totaled 80 individuals; today more than 52,000 TSA personnel serve on the frontlines at over 450 U.S. airports.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00944 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.570

Increased Security at Airport Checkpoints

Through the American Recovery and Reinvestment Act of 2009 and annual appropriations, TSA has accelerated the deployment of new technologies at airports, including Advanced Imaging Technology (AIT) to detect the next generation of threats. In 2008, TSA began deploying AIT units, which resulted in the detection of hundreds of prohibited, illegal or dangerous items at checkpoints nationwide. AIT safely screens passengers for metallic and nonmetallic threats, including weapons, explosives and other objects concealed under layers of clothing. AIT has been evaluated and determined to be safe for all passengers by the Food and Drug Administration, National Institute for Standards and Technology and Johns Hopkins University Applied Physics Laboratory.

TSA ensures passenger privacy through the anonymity of AIT images—a privacy filter is applied to blur facial images; all images examined by TSA at airports are permanently and immediately deleted upon viewing; AIT images are not stored, transmitted or printed; the officer viewing the image never sees the passenger; and the officer assisting the passenger cannot view the image. TSA has begun installing automated target recognition software on millimeter wave AIT units that automatically detects potential threats without the need for screeners to view the AIT image, instead using a generic outline of a person for all passengers—further enhancing the privacy protections in place for AIT screening. Going forward, all millimeter wave AIT units that TSA deploys will include this new software. Backscatter AIT units will also have similar software installations.

TSA utilizes a range of technology to detect explosives at checkpoints, including Explosive Trace Detection units to screen carry-on articles, checked baggage, and passengers for explosive residue; Advanced Technology X-Ray machines that scan carry-on baggage from multiple angles, providing the operator with a clear image regardless of the bag's orientation within the machine; Bottled Liquid Scanners capable of detecting explosives and flammable liquids; and Explosive Detection Systems that screen checked baggage for explosives and can quickly determine if a bag contains a potential threat.

Increased Regulation and Security for Air Cargo

Prior to 9/11, limited federal security requirements existed for cargo screening. Now, in accordance with a Congressional mandate, 100 percent of all cargo transported on passenger aircraft that depart U.S. airports is screened commensurate with screening of passenger checked baggage. This milestone has been accomplished largely through the Certified Cargo Screening Program, which permits entities throughout the air cargo supply chain that have undergone rigorous inspection and certification processes to screen cargo.

In December 2010, TSA implemented requirements for 100 percent screening of high-risk cargo on international flights bound for the United States. DHS is also currently evaluating formal industry comment to a proposal to finalize its timeline for implementing the 100 percent international inbound cargo screening requirement. As part of this effort, TSA will work with

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00945 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.571

industry to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process.

In January 2011, DHS also launched a partnership with the World Customs Organization (WCO) to enlist other nations, international bodies and the private sector in increasing the security of the global supply chain—outlining a series of new initiatives to make the system stronger, smarter and more resilient. The three main elements of this international effort to strengthen the security of the global supply chain include preventing terrorists from exploiting the global supply chain to plan and execute attacks; protecting the most critical elements of the supply chain system, such as transportation hubs and related critical infrastructure, from attacks and disruptions; and building the resilience of the global supply chain to ensure that if something does happen, the supply chain can recover quickly.

As part of the effort to strengthen the global supply chain, ICE, in coordination with WCO, launched Operation Global Shield in 2010, a multilateral law enforcement effort aimed at combating the illicit cross-border diversion and trafficking of precursor chemicals for making improvised explosive devices (IED) by monitoring their cross-border movements. In March 2011, WCO voted to make the newly-renamed Project Global Shield a permanent program.

TSA also deploys canine teams to screen air cargo at the nation's highest cargo volume airports and provides explosives detection capabilities in the aviation, mass transit, and maritime transportation sectors. The TSA National Explosive Detection Canine Team Program has grown from 200 teams in 2001 to 900 teams in 2011. TSA has also developed a Passenger Screening Canine training program to enhance a canine's ability to detect explosive materials in baggage as well as on passengers.

Strengthening Efforts to Detect and Report Biological, Radiological and Nuclear Threats

Countering nuclear, biological, and radiological threats requires a coordinated, whole-of government approach. The Domestic Nuclear Detection Office (DNDO)—formed in 2005 as part of DHS—works in partnership with agencies across federal, state and local government to prevent attacks from radiological or nuclear materials through detection activities and and to deter attacks through forensics programs.

Working with partners from across the Administration, including the Departments of Defense, State, Energy, and Justice, the Intelligence Community, and the Nuclear Regulatory Commission, DNDO helps integrate interagency efforts to develop nuclear detection capabilities, respond to detection alarms, conduct research and development, and coordinate the development of the global nuclear detection architecture (GNDA).

In December 2010, DNDO submitted to Congress the GNDA Strategic Plan, an interagency product designed to guide the nation's nuclear detection capacity and capability development over the next five years. DNDO develops nuclear detection capabilities and implements the domestic portion of the GNDA in coordination with federal, state, local, international, and private sector partners as well as the Department's operational components.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00946 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.572

For example, DNDO has worked with CBP to deploy Radiation Portal Monitors and other radiation detection technologies to seaports, land border ports, and mail facilities around the world. When the Department was formed in 2003, these systems scanned only 68 percent of arriving trucks and passenger vehicles along the Northern border. No systems were deployed to the Southwest border, and only one was deployed to a seaport. Today, these systems scan 100 percent of all containerized cargo and personal vehicles arriving in the U.S. through land ports of entry, as well as over 99 percent of arriving sea containers.

Additionally, DHS has procured thousands of Personal Radiation Detectors, Radiological Isotope Identification devices, and backpack detectors for CBP, USCG, TSA, and state and local law enforcement across the country to scan cars, trucks, and other items and conveyances for the presence of radiological and nuclear materials. DNDO has also made radiological and nuclear detection training available to over 15,000 state and local officers and first responders.

In its fiscal year 2012 budget request, DHS proposed expanding the Securing the Cities (STC) initiative, designed to enhance the nation's ability to detect and prevent a radiological or nuclear attack in the highest risk cities and urban areas while continuing to support efforts in New York. Through STC, nearly 11,000 personnel in the New York City region have been trained in preventive radiological and nuclear detection operations, and nearly 6,000 pieces of radiological detection equipment have been deployed.

DHS is also responsible for advancing the nation's nuclear forensics capability which, in conjunction with law enforcement and intelligence information, supports the identification of individuals involved in planned or actual attacks using radiological or nuclear weapons or materials. In fiscal year 2008, DNDO launched the National Nuclear Forensics Expertise Development (NNFED) Program—a collaborative effort with DOE and DOD to address the critical human capital needs of the technical nuclear forensics community.

One of DHS's highest priorities is preventing terrorist groups and hostile nations from illegally obtaining U.S. military products and sensitive technology, including components of weapons of mass destruction. To this end, ICE established the National Export Enforcement Coordination Network to better coordinate export enforcement efforts among law enforcement agencies and with the intelligence community.

Through another initiative called Project Shield America, ICE conducts outreach to manufacturers and exporters of strategic commodities that are believed to be targeted for procurement by terrorist organizations and the countries that support them, as well as countries identified as weapons proliferators. In November 2010, President Obama issued an Executive Order authorizing the establishment of the Export Enforcement Coordination Center to coordinate and enhance export control enforcement efforts among federal law enforcement agencies, export licensing agencies, and the intelligence community. The center will begin operations in late 2011.

The DHS Office of Health Affairs (OHA) coordinates the department's biological and chemical defense activities, providing medical and scientific expertise to support preparedness and response efforts. DHS S&T's Chemical and Biological Defense Division also works to increase

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00947 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.573

the nation's preparedness against chemical and biological threats through improved threat awareness, and development of advanced surveillance and detection, and responsive countermeasures.

Since the anthrax attacks 10 years ago, DHS also has made great strides in protecting the nation from, and preparing federal, state, and local governments to respond to biological attacks. In 2003, the Department stood up the BioWatch system—a federally-managed, locally-operated, nationwide environmental monitoring system designed to detect the intentional release of aerosolized biological agents which is currently operational in approximately 30 cities. In 2010, the Department began testing the next generation of automated early detection systems, known as Gen-3 which will reduce detection times.

To improve state and local biopreparedness, DHS established the first formalized sharing of public health and intelligence information with state and local health partners in 2009. In 2010, the Department developed and conducted a series of biological attack response exercises, including one in each of the 10 FEMA regions, involving more than 1,000 state and local officials. The Department has also contributed to the physical safety and security of biological select agent facilities by completing Buffer Zone Plans and Site Assistance Visits, and providing grant funding to first responders at these facilities.

Recognizing the critical need to dispense life-saving medical countermeasures to those potentially exposed to aerosolized anthrax spores within 48 hours of exposure, OHA started a program that ensures the Department's mission essential functions by distributing medical countermeasures to personnel serving in critical roles during an emergency.

Through the National Biodefense Analysis and Countermeasures Center (NBACC), S&T continues to provide critical biological threat analysis and forensic capabilities to understand the risks posed by biological threats and to attribute their use in bioterrorism or biocrime events. In addition, S&T supports the Chemical Security Analysis Center (CSAC) to increase awareness of chemical threats and the attribution of their use against the American public. S&T is also leading a joint effort known as the Integrated Consortium of Laboratory Networks (ICLN) to integrate and coordinate laboratory surge capacity in response to a significant chemical, biological, radiological attack or incident.

To save lives and expedite response efforts in the event of a terrorist chemical agent release inside a high-threat facility, DHS S&T also has developed the PROTECT system which is now deployed by jurisdictions through funding provided by the Transit Security Grant Program. PROTECT integrates detection, video surveillance, and operational communication systems for interior infrastructure protection for chemical incidents. In a demonstration, the system reduced the time responders appeared on scene from 30 minutes to 5 minutes

Protecting Cyber Networks and Critical Physical Infrastructure

Cybersecurity

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00948 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.574

Today's threats to cybersecurity require the engagement of the entire society – from government and law enforcement to the private sector and importantly, members of the public – to block malicious actors while bolstering defensive capabilities. DHS leads the whole of government effort to protect the federal executive branch civilian agencies and assisting the protection of the nation's critical infrastructure and critical information systems, where the government maintains essential functions and which provide services to the American people and support the financial services, energy, and defense industries.

In October 2010, DHS and DOD signed a Memorandum of Agreement to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks. The Agreement embeds DOD cyber analysts within DHS and sends a new team of DHS experts to NSA to be supported by DHS privacy, civil liberties, and legal offices.

In November 2010, the Multi-State Information Sharing and Analysis Center, opened the Cyber Security Operations Center, a 24-hour watch and warning facility, to enhance situational awareness at the state and local level and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments.

In partnership with the private sector, the U.S. Computer Emergency Readiness Team (US-CERT) also takes proactive measures to stop possible threats from reaching an even broader audience by developing and sharing standardized prevention, mitigation, and response information products with its government and private sector partners. The DHS Office of Intelligence and Analysis also enables prevention, mitigation, and response through all-source intelligence analysis of cyber threats to federal Executive Branch civilian departments and agencies, state and local governments, and U.S. critical infrastructure and key resources.

Protecting critical infrastructure – including the systems and networks that support the financial services, energy, and defense industries – also requires a full range of partners, including other government agencies, the private sector and individuals. DHS led the development of the first-ever National Cyber Incident Response Plan to coordinate the response of multiple federal agencies, state and local governments, and the private sector to incidents at all levels.

In October 2009, DHS also opened the new National Cybersecurity and Communications Integration Center (NCCIC) —a 24-hour, DHS-led coordinated watch and warning center to serve as the nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture.

DHS also utilizes the National Cybersecurity Protection System, of which the EINSTEIN intrusion detection system is a key component, to protect federal dot-gov domains. When fully deployed, the EINSTEIN system, initially deployed in 2004, will help block malicious actors from accessing federal executive branch civilian agencies, while working closely with those agencies to bolster their defensive capabilities.

Recently, DHS deployed EINSTEIN 2—a detection system that monitors federal internet traffic for malicious intrusions—at 15 Departments and agencies and four Managed Trusted Internet Protocol Service providers. At full operational capability, the next-generation EINSTEIN 3 will

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00949 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.575

provide DHS with the ability to detect malicious activity and disable attempted intrusions automatically, a significant improvement in the Department's ability to prevent cyber intrusions on federal executive branch civilian networks and systems.

Additionally, as part of the Comprehensive National Cybersecurity Initiative, DHS is working to reduce and consolidate the number of external connections that federal agencies have to the Internet through the Trusted Internet Connection (TIC) initiative. This initiative reduces the number of potential vulnerabilities to government networks and allows DHS to focus monitoring efforts and security capabilities on limited and known avenues for Internet traffic. In April 2011, the Obama Administration released the National Strategy for Trusted Identities in Cyberspace (NSTIC), which seeks to secure the identities of individuals, organizations, services and devices during select online transactions, as well as the infrastructure supporting the transaction.

To meet our future workforce needs, DHS is also building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to CIKR. Through its Cybersecurity Workforce Initiative, DHS has increased its cyber staff by 500 percent while working with universities to build the cybersecurity pipeline through competitive scholarship, fellowship, and internship programs to continue to attract top talent. Additionally, DHS S&T co-sponsors national and regional cybersecurity competitions, at the high school and collegiate levels, to educate young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts.

Finally, DHS is committed to increasing public awareness about cybersecurity and empowering individuals and enterprises across cyber networks to enhance their own security operations. In 2010, the Department launched the *"Stop. Think. Connect."* public cybersecurity awareness campaign to increase public understanding of cyber threats and promote simple steps the public can take to increase their safety and security online.

Protecting Critical Infrastructure

Since fiscal year 2006, DHS has provided nearly $4 billion in grant funding through the Port Security, Transit Security and Buffer Zone Protection grant programs to protect critical infrastructure from terrorism. These grants support security plans, facility security upgrades, training, exercises, law enforcement anti-terrorism operations, and capital projects for risk mitigation of high threat infrastructure.

In 2009, DHS revised the National Infrastructure Protection Plan (NIPP) to integrate resilience and protection and broaden the focus of NIPP-related programs and activities to an all-hazards environment. DHS also developed an annual National Risk Profile that provides a multi-hazard assessment of risks facing critical infrastructure, including terrorist threats, cyber risks, and natural disasters.

Since 2007, DHS has implemented the Chemical Facility Anti-Terrorism Standards (CFATS) to regulate security at high-risk chemical facilities. To date, the Department has reviewed an estimated 40,000 consequence assessment questionnaires submitted by potentially high-risk

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00950 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.576

chemical facilities. Of these, approximately 4,500 facilities have been preliminarily identified as high-risk, resulting in the development and submission of Security Vulnerability Assessments. Of those facilities, most have received final high-risk determinations and have submitted or are in the process of completing Site Security Plans for DHS review to determine whether their security measures meet CFATS performance standards.

The Department's Office of Infrastructure Protection (IP) also has conducted more than 1,900 security surveys and more than 2,500 vulnerability assessments of the nation's critical infrastructure to identify security gaps and potential vulnerabilities and to provide protective measures recommendations to enhance the protection and resilience of the nation's critical infrastructure. In addition, IP has conducted more than 1,400 capability assessments of state and local bomb squads, explosives detection canine teams, dive teams, and SWAT teams to identify potential gaps and provide recommendations to mitigate vulnerabilities.

The Department also has deployed Protective Security Advisors (PSAs) to all 50 states, Puerto Rico, and the District of Columbia to support state, local, tribal and territorial officials and the private sector with critical infrastructure security efforts; coordinate and conduct vulnerability assessments and training; respond to all hazard incidents impacting critical infrastructure; and support effective information sharing and situational awareness. Additionally, the DHS S&T Directorate also conducts research and development to create new technologies to enhance critical infrastructure security.

Risk-based Security Grants

To support state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies, since fiscal year 2003, DHS has awarded more than $32 billion in preparedness grant funding based on risk to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism.

DHS continues to focus our grant funding on realizing and sustaining our operational priorities. For example, the fiscal year 2011 Urban Areas Security Initiative (UASI) grants encourage the development and sustainment of baseline capabilities at fusion centers. The UASI Program provides funding to address the unique planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism. Additionally, Transit Security Grant funding is prioritized based on risk and supports "shovel ready" security projects for critical assets.

Further, to address homegrown violent extremism, DHS has prioritized grant-funded prevention activities that directly support local homeland security efforts to understand, recognize, prepare for, prevent and respond to pre-operational activity and other crimes that are precursors or indicators of terrorist activity, while respecting privacy, civil rights and civil liberties protections.

Emergency Communications and Unified Incident Command

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00951 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.577

Since 9/11, DHS has worked to transform and strengthen interoperable communications across the country. Through the establishment of the Office of Emergency Communications, the awarding of more than $4 billion in dedicated grant funding for state and local interoperability efforts, and the development and deployment of new technologies, DHS has helped to enhance coordination to ensure that emergency response providers can communicate during natural disasters, acts of terrorism, and other catastrophic events. Additionally, in 2011, the Obama Administration announced a plan to deploy a nationwide, interoperable wireless broadband network for public safety.

DHS has made significant progress in establishing and improving a unified incident command system to respond to a wide range of threats, from natural disasters to coordinated attacks. The Incident Command System (ICS) provides a flexible mechanism for coordinated and collaborative management for many incidents, covering large or small geographical areas, single or multiple governments, nongovernmental, and/or private sector organizations. FEMA's disaster response operations are also organized along ICS principles. FEMA has established 25 Incident Management Assistance Teams (IMATs) that utilize the ICS as their core organizational management structure.

In 2010, DHS worked with 60 urban areas to assess emergency communications during a real-world situation. All 60 urban areas successfully demonstrated response-level emergency communications. These demonstrations illustrate how the significant organizational and technical investments funded through the Interoperable Emergency Communications and UASI Grants have improved their emergency communications capabilities in recent years.

DHS is also prioritizing private sector preparedness through programs such as the Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep™), Ready Business, the development and deployment of new technologies, and by incorporating private sector partners from the outset when developing new policies, programs and initiatives.

Bolstering the Security of U.S. Borders and Identification Documents

Protecting our nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to the security and economic prosperity of our homeland. Over the past several years, DHS has deployed unprecedented levels of personnel, technology, and resources to the Southwest border. At the same time, DHS has made critical security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure while also strengthening efforts to increase the security of the nation's maritime borders.

Southwest Border

Over the past two years, the Obama Administration has deployed unprecedented levels of personnel, technology, and resources to the Southwest border. Today, the Border Patrol has more staff than at any time in its 87-year history. Along the Southwest border, DHS has increased the number of civilian boots on the ground from approximately 9,100 Border Patrol agents in 2001 to more than 17,900 today.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00952 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.578

Under the Southwest Border Initiative, DHS has doubled the number of personnel assigned to ICE-led Border Enforcement Security Task Forces (BESTs), which work to dismantle criminal organizations along the border; increased the number of ICE intelligence analysts along the border focused on violence caused by transnational criminal organizations; tripled deployments of Border Liaison Officers to work with their Mexican counterparts; begun screening 100 percent of southbound rail shipments for illegal weapons, drugs, and cash; and expanded Unmanned Aircraft System (UAS) coverage to the entire Southwest border. There were no deployments of UASs along the Southwest border prior to 9/11.

Further, the $600 million supplemental funding requested by the Administration and passed by Congress in 2010 has enabled DHS to continue to add technology, personnel, and infrastructure to the Southwest border. These resources include 1,000 additional Border Patrol agents; 250 new CBP officers at U.S. ports of entry; 250 new ICE agents focused on transnational crime; improved tactical communications systems; two new forward operating bases to improve coordination of border security activities; and additional CBP UASs.

While this work is not yet complete, every key metric available shows that these border security efforts are producing significant results. Illegal immigration attempts, as measured by Border Patrol apprehensions, have decreased 36 percent in the past two years, and are less than one third of what they were at their peak. Seizures of drugs, weapons and currency have increased across the board. In fiscal years 2009, 2010, and the first half of 2011, CBP and ICE seized 75 percent more currency, 31 percent more drugs, and 64 percent more weapons along the Southwest border as compared to the same time period during the previous administration. Additionally, violent crime in U.S. border communities has remained flat or fallen in the past decade—in fact, studies and statistics have shown that some of the safest cities and communities in America are along the Southwest border.

In July 2011, the Obama Administration released its most recent National Southwest Border Counternarcotics Strategy, which provides the Administration's overarching framework to address the threats posed by the illicit narcotics trade. DHS has also forged historic agreements with DOJ, increasing coordination between ICE and the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Drug Enforcement Administration (DEA), on important Southwest border issues such as combating arms trafficking, bolstering information sharing and providing ICE agents the authority to work on important drug trafficking cases.

Further, President Obama authorized the temporary use of up to 1,200 additional National Guard personnel as a bridge to longer-term enhancements in border protection and law enforcement personnel from DHS to target illicit networks' trafficking in people, drugs, illegal weapons, money, and the violence associated with these illegal activities. That support has allowed DHS to bridge the gap and to hire the additional agents funded in the FY 2010 Border Security Supplemental to support efforts along the Southwest border.

In partnership with DEA and DOD, the Administration established the new Border Intelligence

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00953 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.579

Fusion Section within the El Paso Intelligence Center, which provides a comprehensive Southwest Border Common Intelligence picture, as well as real-time operational intelligence, to law enforcement partners in the region—further streamlining and enhancing operations.

The federal government has continued to work closely with state and local law enforcement along the border, serving together on task forces, conducting joint operations, providing the latest intelligence, and coordinating operational priorities.

Reflecting unprecedented collaboration, DHS and its Mexican counterpart agencies have signed numerous bilateral agreements and declarations to bolster and deepen collaboration and coordination in the areas of enforcement, planning, information sharing, and trade facilitation along the Southwest border. DHS works in partnership with DOS, DOJ and Mexico to implement Presidents Obama and Calderon's Declaration on 21st Century Border Management, pursuing initiatives and programs designed to expedite the legitimate flow of people and goods and focus law enforcement resources on those people and goods that represent the highest risk.

Northern Border

The Obama Administration has made significant advancements in creating a secure and resilient Northern border. DHS continues to invest in personnel, technology, and infrastructure, and to strengthen cooperation with federal, state/provincial, tribal, and private sector partners on both sides of the border. These achievements have resulted in a more secure Northern border that facilitates legitimate travel and trade.

DHS has made important security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure. Currently, CBP has more than 2,200 Border Patrol agents on the Northern border, a 500 percent increase since 9/11. CBP also has nearly 3,700 CBP officers managing the flow of people and goods across ports of entry and crossings along the Northern border. In addition, CBP is using Recovery Act funds to modernize more than 35 land ports of entry along the Northern border to meet current security and operational needs.

The Department has also continued to deploy technology along the Northern border, including thermal camera systems, Mobile Surveillance Systems, and Remote Video Surveillance Systems, and successfully completed the first long-range CBP Predator-B unmanned aircraft patrol under expanded Federal Aviation Administration authorization that extends the range of approved airspace along the Northern border. Approximately 950 miles along the Northern border from Washington to Minnesota are currently covered by unmanned aircraft, in addition to approximately 200 miles along the northern border in New York and Lake Ontario—none of which were covered prior to the creation of DHS.

In February 2011, President Obama and Canadian Prime Minister Harper announced a landmark "Shared Vision for Perimeter Security and Economic Competitiveness" that sets forth how the two countries will manage shared homeland and economic security in the 21st century. This "Shared Vision" focuses on addressing threats at the earliest point possible; facilitating trade,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00954 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.580

economic growth, and jobs; collaborating on integrated cross-border law enforcement; and partnering to secure and strengthen the resilience of critical infrastructure and cybersecurity.

As the lead agency for maritime border security, the USCG works with other federal, state, local and tribal partners to enhance security along the U.S. maritime border and uses interagency partnerships and international bilateral agreements to accomplish this mission. The USCG's overarching strategy is to improve maritime border security through a layered security system that begins beyond the country's physical borders. At-sea presence deters potential threats, provides mobile surveillance coverage, increases warning time, engages smugglers before they reach our shores, and enables USCG to address potential threats before they can cause harm to the United States.

Identification Documents and Biometrics

DHS has taken significant steps to strengthen security, reduce fraud and improve the reliability and accuracy of personal identification documents while enhancing privacy safeguards. This includes fundamentally transforming the way travelers enter the United States from within the Western Hemisphere through implementation of the Western Hemisphere Travel Initiative (WHTI) and from other countries around the world through the VWP, VSP and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program biometric identity and verification process.

In 2009, DHS implemented WHTI at land and sea ports of entry to strengthen border security for entry to the U.S., while facilitating legitimate travel and trade. WHTI requires that U.S., Mexican, Canadian and Bermudan citizens present a passport or other designated, secure travel document that denotes identity and citizenship when seeking to enter the United States. Prior to the implementation of WHTI, there was no documentary requirement for U.S. or most Canadian citizens to enter the United States from within the Western Hemisphere; travelers could present any one of numerous documents or simply make an oral declaration of citizenship. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases. Today, due to WHTI, 97 percent of travelers are compliant with WHTI.

As noted earlier, DHS implemented ESTA in 2008 to screen VWP program applicants prior to travel to the United States and, as a result, has generally automated the arrival/departure form (Form I-94W) for authorized travelers arriving at airports or seaports from VWP countries. Through the Visa Security Program, which did not exist on 9/11, ICE, with Department of State concurrence, deploys trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States.

The US-VISIT biometric identity verification process collects digital fingerprints and a photograph from international travelers at U.S. visa-issuing posts and ports of entry to help Department of State officials determine whether a person is eligible to receive a visa and to assist CBP officers at ports of entry in determining whether a foreign national may enter the United States. This information is screened against the US-VISIT's IDENT database, a biographic and biometric repository, and is matched with biometric data collected previously from the person,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00955 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.581

such as during a visa application, or a prior entry into the United States, to confirm whether the person is using his/her established identity.

To date, DHS has achieved ten-fingerprint identity verification for 99 percent of air and sea points of entry. Prior to 9/11, there was no capability to verify a visitor's claimed identity beyond a visual check of their identification documents.

DHS is also undertaking a Department-wide effort to address the backlog of unvetted potential visa overstays, an issue identified by the U.S. Government Accountability Office (GAO) in its April, 2011 report. The goal of this ongoing effort is not only to identify which individuals have overstayed their visas, but also to prioritize for removal identified overstays who may be a threat to national security.

In addition, USCIS continues to enhance fraud detection and national security capabilities to ensure that immigration benefits are not granted to individuals who pose a threat to national security. USCIS has embedded Fraud Detection and National Security officers in eight other government agencies to increase information sharing and collaboration efforts that enhance law enforcement and intelligence operations. Further, USCIS has implemented a new state-of-the-art system that enhances the verification and sharing of electronic records and has redesigned all of its secure identity documents to comport with the latest DHS and International Civil Aviation Organization standards as well as best practices in industry and government.

Since 2009, USCIS has incorporated the use of electronic fingerprints in all of its overseas programs to enhance the accuracy and effectiveness of its verification checks. The new Permanent Resident Card (commonly referred to as a "green card"), implemented in 2010, includes new security features that reduce the risks of counterfeiting, tampering, and fraud; it also includes a radio frequency identification tag that serves as a pointer to a record in a secure DHS database. USCIS has also updated the Employment Authorization Document, known as "work permit," by adding a machine-readable zone.

Since 2007, DHS also has enrolled over 1.9 million port workers and merchant mariners in the Transportation Worker Identification Credential (TWIC) program, and issued a tamper-resistant biometric credential to those who require unescorted access to secure areas of ports and vessels and who were determined not to present a security risk.

Additionally within the maritime domain, the USCG has implemented a mobile biometrics collection system to identify undocumented migrants and match them against known databases of past criminal and immigration violations as well as terrorist watchlists, enabling the USCG to prosecute repeat offenders. Through June 2011, the USCG has identified more than 900 individuals who were enrolled in US-VISIT's IDENT biometric database as prior felons, violators of U.S. immigration laws, or other persons of interest and referred them to law enforcement authorities for appropriate action.

Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00956 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.582

DHS has the first statutorily required privacy office of any federal agency, and the Department builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development.

The DHS Privacy Office partners with every DHS component to assess policies, programs, systems, technologies, and rulemakings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information.

DHS's Office for Civil Rights and Civil Liberties (CRCL) plays a key role in the Department's mission to secure the nation while preserving individual freedoms and represents the Department's commitment to the idea that core civil rights values – liberty, fairness, and equality under the law – are a vital part of America, and that these values provide a bulwark against those who threaten our safety and security. Since its inception, CRCL has expanded its participation in programs and activities throughout the Department and continued its efforts to promote civil rights and civil liberties.

CRCL's community engagement efforts include a wide variety of stakeholders and organizations through regular roundtables across the country. CRCL has also expanded its training capacity and worked closely with the DHS Privacy Office and the Office of Intelligence and Analysis to offer civil rights and civil liberties training for fusion centers, as well as training to a number of the Department's federal, state, and local partners.

Challenges that Remain

While DHS has made great progress in securing the nation since the September 11, 2001 attacks, challenges remain in implementing key recommendations in the 9/11 Commission Report.

Despite significant efforts, including the proposed PASS ID legislation to enhance the security of driver's licenses, many states are still unable to fulfill the congressionally mandated REAL ID requirements. The Department also continues to undertake new steps to increase the use of risk based security screening; develop strategies to guard against an increasing volume of cyber attacks; partner with first responders to address interoperability challenges; and determine a cost-effective means to implement a biometric exit solution.

While the demands on DHS have never been greater, the current fiscal climate requires the Department to continue to maximize every security dollar. In order to preserve front line security operations, DHS has identified over $1 billion in cost avoidances and cuts under this Administration. In addition, the Department's fiscal year 2012 budget request included more than $800 million in further reductions associated with administrative savings and efficiency initiatives currently underway, from efforts to reform acquisition, asset and real property management to cuts to professional services contracts, supplies and materials, printing, and travel.

Additionally, it is my hope that Congress will address an unmet 9/11 Commission recommendation that is solely within its power to solve. Effective congressional oversight is critical to promoting transparency, accountability and efficiency. The 9/11 Commission Report

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00957 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.583

recognized that the existing structure of fragmented and disparate oversight over DHS requires significant department resources and hinders Congress's ability to provide the department with clear oversight and guidance. We can all agree that reforming this system will be good for Congress, DHS and the American people.

Conclusion

While America is stronger and more resilient as a result of these efforts to strengthen the homeland security enterprise, threats from terrorism persist and continue to evolve. Today's threats do not come from any one individual or group. They may originate in distant lands or local neighborhoods. They may be as simple as a homemade bomb or as sophisticated as a biological threat or coordinated cyber attack.

Increasingly, state, local, and tribal law enforcement officers, as well as citizens, businesses, and communities are on the frontlines of detection and prevention. Protecting the nation is a shared responsibility and everyone can contribute by staying informed and aware of the threats the country faces. Homeland security starts with hometown security—and we all have a role to play.

I want to thank Congress – and this Committee in particular – for your role in the creation of the Department, your continued support for our critical efforts, and your invaluable guidance and oversight as we continue to work to create a stronger and safer country.

I have stated before that we cannot put our country under a glass dome or guarantee we will never again face another terrorist attack. But we will do everything within our power to secure our nation against a large attack or disaster, to protect critical infrastructure and cyber networks, and to continue to engage a broader range of Americans in our shared responsibility for security. I look forward to any questions you may have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00958 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.584

Department of Justice

STATEMENT OF

ROBERT S. MUELLER III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

"TEN YEARS AFTER 9/11: ARE WE SAFER?"

PRESENTED

SEPTEMBER 13, 2011

STATEMENT FOR THE RECORD OF
ROBERT S. MUELLER III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"TEN YEARS AFTER 9/11: ARE WE SAFER?"

PRESENTED
SEPTEMBER 13, 2011

Good morning, Chairman Lieberman, Ranking Member Collins, and Members of the Committee. Thank you for the opportunity to appear before the Committee today to discuss the threats facing our nation and the efforts of the FBI to protect the United States over the past ten years.

Introduction

The mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to Federal, State, municipal, tribal, and international agencies and partners. The FBI's number one priority in this mission continues to be the prevention of terrorist attacks against the United States. To improve its ability to detect and disrupt those with the intent and capability to conduct attacks in the United States, the FBI has undergone a paradigm shift in the way we collect and use intelligence.

The FBI significantly increased its intelligence capacity after the attacks of September 11, 2001, when the FBI elevated counterterrorism to its highest priority. Prior to the 9/11 attacks, the FBI's operations were heavily weighted towards its law enforcement mission; intelligence tools and authorities were primarily used for the counterintelligence mission. In the immediate aftermath of 9/11, the FBI quickly identified the need to enhance intelligence programs with improved analytical and information sharing capacities to detect and prevent future terrorist attacks.

Protecting the United States against terrorism demanded a new framework for the way the FBI carries out its mission: a threat-based, intelligence-led approach. Rather than collecting information to solve a particular case, the new approach prioritizes the collection and utilization of intelligence to develop a comprehensive threat picture, enabling strategic disruptions of

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00960 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.586

terrorist networks before they act. This focus on the overall threat picture also elevates the need for information sharing, thereby changing the FBI's role in and relationships with both the intelligence and law enforcement communities. Under this new model, intelligence drives how we understand threats, how we prioritize and investigate these threats, and how we target our resources to address these threats.

This new approach has driven significant changes in the Bureau's structure and management, resource allocation, hiring, training, recruitment, information technology systems, interagency collaboration and information sharing, as well as a paradigm shift in the FBI's cultural mindset. These changes have transformed the Bureau into a national security organization that fuses traditional law enforcement and intelligence missions. At the same time, the FBI remains vigilant in upholding the Constitution, the rule of law, and protecting privacy rights and civil liberties.

Today's FBI: A National Security Organization

In the years since 9/11, the FBI has integrated its intelligence mission with its traditional law enforcement mission, enhancing its ability as a national security organization. Like other intelligence agencies, the FBI collects, exploits, disseminates, and analyzes intelligence. The FBI combines these functions to collect and act on intelligence as a national security organization. As a result, the FBI is not solely an intelligence or law enforcement agency. The FBI's actions are not limited to arrests and prosecutions; they take many forms, including recruiting potential intelligence sources; developing new collection requirements (pieces of information sought to complete a particular threat picture); and supporting our Federal, State, local, and tribal partners to exercise their distinct authorities to disrupt plots before they cause harm.

The FBI has a long history of collecting intelligence to be used as evidence to dismantle criminal networks or to identify and prosecute spies. Historically, information was collected with a goal of using it to drive traditional law enforcement action: arrest and prosecution. However, being driven by threat rather than arrest and prosecution means prioritizing intelligence collection. Under the FBI's new paradigm, intelligence enables a broader picture of the threat. Intelligence is not collected simply to further a particular case. This shift required the integration of intelligence and law enforcement capabilities. Intelligence is analyzed and disseminated to better understand the threat, to identify intelligence gaps, and to develop new collection requirements, which drive additional action in the field, leading to either additional collection or disruption. It is this continuous intelligence cycle that drives investigative strategies to ensure resources are targeting the most pressing threats.

Another key element of the FBI's evolution into an effective national security organization has been augmenting relationships and information sharing with the United States Intelligence Community ("the Intelligence Community"), as well as Federal, State, local, tribal, and foreign law enforcement partners. The Bureau has accomplished this interconnectivity

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00961 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.587

through the development of and participation in joint operational programs and task forces, expansion of our presence overseas, and the development of information technology systems that support information sharing. Meeting the requirements of the intelligence cycle necessitated a significant enhancement of the Bureau's intelligence capacity and expertise.

Building the Structure and Management Capability for a National Security Organization

The Initial Steps of the Transformation

To meet the immediate demands of the post-9/11 threat environment, the Bureau shifted resources from criminal investigations to national security matters, adding almost 2,000 agents to its national security programs within one year. Soon thereafter, the FBI began the process of creating a national security focus and aligning the organization to address this priority. One of the first steps was to centralize control and management of counterterrorism operations at Headquarters to avoid the "stove-piping" of information on terrorism cases in the 56 individual Field Offices across the country. Another was building the critical intelligence infrastructure to meet the needs of production and dissemination of intelligence products. The building blocks of this infrastructure included: establishing an intelligence office at Headquarters; creating a Field Intelligence Group (FIG) for each Field Office across the country; augmenting counterterrorism resources at Headquarters; hiring more intelligence and language analysts; creating systems to enable more efficient search and analysis capability; and developing new training.

As the various elements of the national security architecture grew both at Headquarters and in the field, a need to focus on and centralize not only counterterrorism operations, but also the Bureau's overall national security mission emerged. This led to the creation of the National Security Branch (NSB) in 2005, which combined the missions, capabilities, and resources of all of the national security components of the Bureau - counterterrorism, counterintelligence, intelligence and weapons of mass destruction. In addition to managing the NSB's internal components, the Executive Assistant Director for NSB -(EAD/NSB) serves as the Bureau's lead intelligence official and representative to the Intelligence Community. With centralized management, the FBI's national security functions have matured internally and the NSB has further integrated itself into the Intelligence Community. To accelerate this integration, NSB created an Associate Executive Assistant Director position that is filled by a senior official from the Intelligence Community. The NSB also has administrative responsibility for two interagency groups: the High-Value Detainee Interrogation Group (HIG) (formally chartered in 2010) and the Terrorist Screening Center (TSC) (formally chartered in 2003).

Management Approach to Lead the Transformation: Strategy Management System (SMS)

While identifying the objective for and building the components of an intelligence-led organization were key steps in the FBI's transformation, transitioning this new threat-based

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00962 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.588

intelligence-led model into practice required additional focus and attention from management. The challenge was to get the network of offices and personnel across the country and around the globe to accept a new mindset and approach to day-to-day operations. The Bureau developed a tool – the Strategy Management System (SMS) – based on the well-regarded balanced scorecard methodology, to measure the execution of its strategy and the progress of its transformation. The SMS is a method to communicate the FBI's strategy, prioritize initiatives, identify each component's role in pursuing the strategy, and measure progress. The core of the strategy is the intelligence cycle. The SMS lays out objectives in each of four categories: the expectations of the American public, internal processes, talent and technology, and resources against which objectives, measures, and initiatives are balanced. Through this structure, the SMS has helped to integrate intelligence into all aspects of the FBI's mission. The SMS used at the Headquarters level cascades down to SMS at the Branch and Division level, thereby creating a cohesive plan under which every component of the Bureau, down to each employee, has a defined role in achieving the goals of the organization. Moreover, to ensure that the FBI's national security mission is aligned with the greater Intelligence Community's mission, NSB's strategy is linked to both the FBI Enterprise-wide strategy as well as the National Intelligence Strategy.

SMS reviews are conducted quarterly at the Executive management level to review progress against the FBI's strategy and at the Branch and Division levels to monitor the execution of the strategy, establish accountability for performance, and ensure alignment with the FBI corporate strategy. The SMS is also linked to and guides the core business processes within the FBI, including: the inspections process, the risk-based management process, spend plan reviews, major resource decisions, and executive performance plans.

Accelerating the Transformation: Strategic Execution Team (SET)

In 2007, recognizing that intelligence had not yet become central in FBI operations and to accelerate the growth of the Bureau's intelligence cycle capabilities, the FBI formed a Strategic Execution Team (SET) initially comprised of almost 100 Special Agents, Intelligence Analysts, and other skilled professionals from Field Offices and FBI Headquarters. The SET examined the intelligence activities in each of the 56 Field Offices and identified two overarching impediments to transformation: integrating intelligence into operations in the field and building human capital for enhanced intelligence capabilities. For example, the SET found that while each Field Office had a FIG, many of the intelligence analysts were being utilized to support the tactical needs of individual cases, rather than being the engine driving strategic collection requirements and, in turn, operations. Following the recommendations of the SET, the FBI standardized the structure and responsibilities of the FIGs to increase collaboration between intelligence and operations, and to provide accountability for intelligence collection, analysis, use, and production. In response to the need to build human capital, the FBI also devoted resources to recruiting and training an analytical workforce that could fulfill the critical functions of the intelligence cycle.

The SET also identified the need for a standardized intelligence role for the operational divisions at Headquarters, similar to the FIGs. SET designed Central Strategic Coordinating

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00963 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.589

Components (CSCCs), where teams of intelligence personnel are embedded in each of the operational divisions to fulfill the primary functions of the intelligence cycle and to improve coordination between the Field Offices and Headquarters components.

Tracking the Progress of the Transformation: Strategy Performance Sessions (SPS)

To better track and measure the Field Offices' progress towards a truly threat-based, intelligence-led approach, in 2008, management at Headquarters began conducting Strategy Performance Sessions (SPS) with Field Offices to review the Field Offices' intelligence and operational performance. The sessions, conducted on a bi-annual basis[1] by secure video teleconference with executives from Headquarters and the management team from two to four Field Offices, focus on: the top threats by operational program facing each Field Office's area of responsibility, or domain; the gaps in intelligence against those top threats; and the strategy to fill those intelligence gaps. The purpose of the SPS is to provide a forum for strategic dialogue, which enables informed decision-making, enhances intelligence and investigative program performance, and instills a culture of accountability. Through SPS sessions, Headquarters divisions gain better insight into the challenges Field Offices are facing in their areas of responsibility and use this knowledge to allocate resources strategically and assist the Field Offices to focus on the cases with the potential to neutralize the greatest threats while recruiting sources who have answers to the most pressing questions. Utilizing the SPS sessions, management has systematically led the cultural transition from a Bureau focused on cases and successful prosecutions to an intelligence-driven organization focused on comprehensive domain awareness and network disruptions.

Human Capital Development

The FBI's current intelligence-led operational model relies in large part on analysts and language specialists who can quickly and effectively review, analyze, and disseminate the intelligence collected in the field. Post 9/11, the FBI's challenge was to develop an intelligence analyst and language specialist cadre that could match the collection capabilities of the Special Agents. The creation of a workforce with the intelligence expertise necessary for today's threats and those of the future required the Bureau to recruit beyond law enforcement and the military communities in order to attract individuals with a broader range of skill sets and advanced degrees in relevant fields. Furthermore, the traditional operational approach created a culture that emphasized the value of Special Agents. This necessitated a strategy that would elevate the stature of analysts. The FBI is meeting this two-part challenge by developing a targeted recruitment strategy, creating rewarding career paths for intelligence analysts, enhancing training programs, and establishing a Leadership Development Program.

---

[1]SPS were originally conducted on a quarterly basis. In 2009, in an effort to reduce the administrative workload on the Field Offices, the frequency was reduced to twice yearly.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00964 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.590

Developing an Intelligence Analyst Cadre

Soon after 9/11, the FBI recruited experienced intelligence analysts from other agencies and students with critical skill sets from universities around the country. The FBI also created opportunities for entry-level positions with career paths that often lead to FBI Intelligence Analyst or Special Agent positions. Since 2001, the FBI has nearly tripled the number of IAs to 3,118, increased the SIA cadre to 285, and increased the number of GS-15 level analysts to 80. This increase in the quantity has been accompanied by a dramatic increase in the capabilities and expertise of the analyst corps. Today, almost half of the FBI's Special Agents were hired post-9/11, and have "grown up" in the intelligence-led culture of today's FBI working side-by-side with analysts.

The FBI has instituted programs to enhance the stature of and career options for analysts. In 2010, the NSB created three analyst career paths - tactical, collection/reporting, and strategic. By defining specific analyst functions, the FBI is creating a specialized, analytic workforce with the appropriate training, experiences, and opportunities for career development. Since 2005, 133 FBI agents and analysts have been certified as Intelligence Officers through the FBI Intelligence Officer Certification Program.

Analysts now also hold Senior Executive Service (SES)-level leadership positions at Headquarters to manage a range of programs, including the CSCCs and the newly established Intelligence Watch. Starting in 2009, the Bureau began establishing Senior Supervisory Intelligence Analyst (SSIA) positions, which are the equivalent of Assistant Special Agents in Charge. SSIAs also perform a full range of managerial and liaison responsibilities with authority over strategic planning activities and personnel matters.

Training is another key element of cultivating a professional analyst workforce. In 2009, the FBI produced a five-year training strategy for Intelligence Analysts, which identified the need for new courses, instructors, and funding. Since then, the FBI's Training Division has been working directly with training units in the NSB to drive training requirements for Intelligence Analysts.

Leadership Development Program

The FBI has a long history of hiring individuals with strong leadership skills, but the fast-paced and continuous changes in the organization created the need for an accelerated and enhanced leadership development program for all employees. In response, in 2009, the FBI established the Leadership Development Program (LDP), the first comprehensive, coordinated approach to leadership in the Bureau's history. LDP's primary goal is to ensure that FBI employees are fully prepared to lead before they assume leadership positions. The LDP's programs, which are at various stages of development and piloting, will deliver a range of programs designed around a leadership doctrine that emphasizes character, courage, competence, and collaboration. LDP's programs will be available to all employees in all locations across the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00965 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.591

Bureau from the day they are hired to the day they retire. Initially, programs are being offered to new employees; employees interested in becoming supervisors; and current supervisors and senior managers. Through its commitment to building the infrastructure to fully implement and sustain the LDP, the FBI will ensure that its employees are prepared to confront current and future challenges and threats.

Supporting the Core Functions of the Intelligence Cycle

The priority of staying ahead of the threat has changed the demand for intelligence as its utility expanded from supporting a particular case to identifying and understanding a broader picture of the threat. This shift required the integration of intelligence and law enforcement capabilities. Intelligence is analyzed and disseminated to better understand the threat, to identify intelligence gaps, and to develop new collection requirements, which drive additional action in the field, leading to either additional collection or disruption. It is this continuous intelligence cycle of collection, integration and dissemination, analysis, and action that drives investigative strategies to ensure resources are targeting the most pressing threats.

Intelligence Collection

Collection of intelligence is conducted by the FBI's greatest asset: its people. Since 9/11, the FBI has more than doubled the number of agents and analysts assigned to its national security mission from 3,537 (2,514 agents/1,023 analysts) to 7,933 (4,815 agents/3,118 analysts). The FBI has a network of personnel spread around the globe with 56 Field Offices and 399 resident agencies domestically, and 62 International Legal Attaché offices around the world which support the collection of raw intelligence.

The Joint Terrorism Task Forces (JTTFs) are interagency squads dedicated to investigating terrorism matters and coordinating counterterrorism efforts across the United States. The FBI has increased the number of JTTFs from 35 in 2001 to 104 today -- one in each of the 56 Field Offices and 48 of the Resident Agencies across the country. In addition to FBI agents, the JTTFs are comprised of Task Force Officers (TFOs) from 32 Federal and 671 State, local, and tribal law enforcement and intelligence agencies. A single National Joint Terrorism Task Force (NJTTF) was created at Headquarters to manage the JTTFs around the country and to provide a venue for collaboration with Intelligence Community personnel to exchange information, analyze data, and plan counterterrorism strategies.

Each of the FBI's 56 Field Offices has a Field Intelligence Group (FIG) composed of Intelligence Analysts, Special Agents, and Staff Operations Specialists (SOS). FIGs, which did not exist prior to 2001, now have 1,662 Intelligence Analysts, 451 Special Agents, and 415 SOSs. The mission of the FIGs is to identify the threats in their respective territories and develop "domain awareness" through collecting, exploiting, analyzing, and disseminating intelligence.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00966 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.592

Intelligence-driven investigations require a unity of effort with partners overseas, especially as global cooperation becomes increasingly necessary to combat terrorism. Through the 62 Legal Attaché offices around the world (an increase of 18 since 2001), the FBI has strengthened relationships with international partners. This expanded global reach not only benefits FBI's foreign partners, but also aids FBI collection efforts and investigations.

The FBI has a leading role in HUMINT collection in the United States. Simply defined, HUMINT is information learned from individuals. People are an invaluable source of intelligence and FBI Special Agents have a long history of developing human sources to uncover criminal conduct and foreign intelligence activities. With the expanded national security mission, the need for and value of HUMINT in understanding our adversaries and developing the threat picture has increased significantly. FBI Headquarters develops policies, training and oversight to ensure adherence to policy directives, and to ensure that information collected is accurate, authentic, reliable, free of undisclosed influence, and consistent with mission objectives across all FBI programs.

Collecting intelligence through physical surveillance is also critical for monitoring threats to our national security. The FBI's Physical Surveillance Program, which was consolidated into one division in 2010, consists of both armed and unarmed Mobile Surveillance Teams and the Field Aviation Program. The armed teams conduct surveillance of armed and dangerous counterterrorism and criminal targets with a propensity for violence. To meet the growing demand for surveillance, the Bureau has increased the number of unarmed surveillance teams by 127% since 2001.

Forensics is another critical source of intelligence. The FBI has earned a global reputation of having premier forensic examiners. Working with interagency partners, the FBI is applying and expanding upon traditional forensic capabilities in support of the counterterrorism mission. The FBI also leads an interagency group based at the FBI Laboratory in Quantico, Virginia, that supports DOD operations in Iraq and Afghanistan: the Terrorist Explosive Device Analytical Center (TEDAC). Established in 2003, funded primarily by the Department of Defense's Joint IED Defeat Organization (JIEDDO), TEDAC is staffed by approximately 230 fulltime government and contract personnel who coordinate and manage a unified intelligence, military, and law enforcement effort to examine improvised explosive devices (IEDs) that are of interest to the United States.

The FBI's use of Foreign Intelligence Surveillance Act (FISA) authorities is an important component of intelligence collection which is subject to a comprehensive oversight and compliance regime in which all three branches of government play a role. The Foreign Intelligence Surveillance Court (FISC) ensures that Constitutional and statutory requirements are met related both to authorization and implementation of the use of the authorities. The Department of Justice's National Security Division, in conjunction with the FBI's Office of the General Counsel, conducts oversight of the FBI's use of FISA authorities to ensure compliance both with the statute and minimization procedures. And, on a semi-annual basis, the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00967 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.598

Government must report to Congress on its use of FISA electronic surveillance, physical search and pen register and trap and trace authorities and submit a detailed annual report on its use of the business record authority.

Publicly available information is also an invaluable source of intelligence that is often overlooked by intelligence analysts in favor of classified or law enforcement sensitive information. Recognizing a need to include open source information in intelligence analysis, the Director of National Intelligence created an Open Source Center (OSC) in 2005. As part of its efforts to strengthen the open source community, the OSC has detailed an Open Source Officer to the FBI for a year to help the Bureau build its own open source program.

Intelligence Analysis and Dissemination

Intelligence collection is only valuable if it is integrated, analyzed, and disseminated effectively and efficiently. As the Bureau has increased its intelligence collection, it has simultaneously developed the capability to exploit and share it. This function resides with the FIGs. The analysts and agents in the FIGs collect raw intelligence from various sources, including agents in the field and intelligence disseminated by other agencies. Analysts then disseminate the raw intelligence and/or create finished intelligence products for dissemination. Developing an analyst corps was only part of the solution to the Bureau's need to increase intelligence dissemination and production. The analysts also needed the necessary information technology and analytic tools to succeed.

To streamline the dissemination of intelligence contained in Intelligence Information Reports (IIRs), the FBI developed an information technology solution, the Collection Operations and Requirements Environment (CORE). CORE standardizes intelligence reporting across the FBI while integrating field intelligence operations with intelligence community requirements. An additional web-based software application, IIR Dissemination System, streamlines, standardizes, and tracks the production of IIRs, and has improved the Bureau's ability to effectively support our Intelligence Community partners. Since 2004, FBI dissemination of IIRs has increased dramatically, providing critical information to the Intelligence Community, law enforcement community, and policymakers.

The FBI continues to develop information technology solutions to minimize the time that intelligence analysts spend searching for relevant information, allowing them to focus on connecting the dots and analyzing the available information. The Data Integration and Visualization System (DIVS) is the FBI's consolidated, enterprise platform that further enhances both the search capabilities and the breadth of information that can be accessed through a single sign-on. DIVS will unify all data accessible to the FBI -- intelligence, criminal investigative, and other mission data -- through one user-friendly search interface, consistent with all applicable legal requirements pertaining to the data. Currently, DIVS houses records from the 11 FBI and other Government agency data sources identified by users as most critical to the FBI's

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00968 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.594

counterterrorism mission. The FBI continues to roll-out this system across the FBI and to add datasets and user tools to provide additional functionality. DIVS is built on a modern platform that will easily expand to integrate tools developed internally, by private industry, or by Intelligence Community partners.

Integration into the United States Intelligence Community and Partnerships with Federal, State, Local, and Tribal Law Enforcement

Another key element of the FBI's evolution into an effective national security organization has been augmenting relationships and information sharing with the United States Intelligence Community, as well as Federal, State, local, tribal, and foreign law enforcement partners. The Bureau has accomplished this interconnectivity through the development of and participation in joint operational programs and task forces, expansion of our presence overseas, and through the development of information technology systems that support information sharing.

As mentioned previously, JTTFs are the primary vehicle by which the Intelligence Community and Federal, State, local, and tribal law enforcement are integrated with domestic counterterrorism operations. The JTTFs currently have almost 2,000 non-FBI employees (approximately 44% of all JTTF members). The FBI's integration with the Intelligence Community is further enhanced by joint duty detailee programs through which law enforcement and intelligence professionals from other agencies are embedded in FBI units and FBI employees are embedded in other agencies. Having professionals from different agencies performing their missions side-by-side has broken down communication barriers and enhanced the mutual understanding of each agency's unique contributions to the community.

Currently, the FBI has more than 200 employees working at other Intelligence Community agencies including the Office of the Director of National Intelligence, the NCTC, the Central Intelligence Agency, the Department of Defense, the Department of Homeland Security, the National Security Agency, and the Department of State. NSB employees also fill intelligence-related positions at the National Security Staff at the White House. Similarly, many of the detailees from other agencies work at joint operational entities administratively located within the FBI, such as the Terrorist Screening Center (TSC), the High-Value Interrogation Group (HIG), the Foreign Terrorist Tracking Task Force (FTTTF), and the National Cyber Investigative Joint Task Force (NCIJTF). These joint operational components along with other joint duty assignments and the EAD/NSB's sustained interaction with the Director of National Intelligence ensure that the FBI is a full partner in the Intelligence Community.

In support of the DNI's effort to create a single IC enterprise that is coordinated, integrated, agile, and effective, the FBI and the ODNI piloted, and are in the process of institutionalizing, a Domestic DNI Representative program. Domestic DNI Representatives are senior field FBI officials at designated offices across the United States who serve as the DNI's

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00969 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.595

principal domestic representative to the IC within their respective areas of responsibility. This program supports the DNI's mission of integrating foreign, military, and domestic intelligence in defense of the homeland and in support of United States national security interests at home and abroad.

Since 9/11, the FBI has evolved to respond to the complex and far-ranging threats we face today. The FBI collects, exploits and disseminates more intelligence to a greater and more useful extent than ever before. This focus on intelligence has helped prioritize our top threats and increased our understanding of our vulnerability to those threats. As the FBI has undergone this transformation, it has remained vigilant in upholding the Constitution, the rule of law, and protecting privacy rights and civil liberties.

Conclusion

Chairman Lieberman and Ranking Member Collins, I would like to conclude by thanking you and this committee for your service and support. I look forward to working with the Committee to improve the FBI as our transformation continues in the future.

I would be happy to answer any questions that you may have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00970 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.596

Hearing Before the Senate Committee on Homeland Security and Governmental Affairs

"Ten Years After 9/11: Are We Safer?"

The Honorable Matthew G. Olsen
Director
National Counterterrorism Center

September 13, 2011

I. Introduction

Chairman Lieberman, Ranking Member Collins, members of the Committee, thank you for the opportunity to appear before you today—along with Homeland Security Secretary Napolitano and FBI Director Mueller—to discuss the evolution of the terrorist threat facing our nation over the last decade and how we are addressing that threat. I also want to thank the Committee for your support of the National Counterterrorism Center, and for the strong working relationship this Committee has developed with NCTC.

It is appropriate that we continue this week to reflect on the day that our nation suffered the single most destructive terrorist attack in our history. In so doing, we honor those who perished and the sacrifices made by the families and loved ones left behind.

The Committee's hearing is entitled, "Ten Years After 9/11: Are We Safer?" The short answer to that question is "yes." While al-Qa'ida and its affiliates continue to pose a significant threat, we are safer than we were on September 11, 2001. Thanks to the skill and hard work of thousands of dedicated men and women in the intelligence, homeland security, diplomatic, and law enforcement communities—as well as our men and women in uniform—we have made significant progress in the fight against terrorism.

With the support and guidance of Congress, we have built an enduring counterterrorism framework by creating new institutions to address terrorist threats. This framework—including the National Counterterrorism Center (NCTC)—has increased the sharing of terrorism-related information within the government, and between federal, state, local and tribal law enforcement, as well as with the public. The government has prevented attacks by disrupting terrorists in the United States and abroad, and prosecuting those arrested for supporting terrorists or their operations. The United States has worked with its partners internationally to promote governance and deny safe haven to terrorists, as well as to counter the flow of funds to terror groups, including designating terrorist entities to cut off funding worldwide.

Al-Qa'ida as an organization is weakened. We have placed relentless pressure on its leadership and worked to deny it safe haven, resources, and the ability to plan and train. Usama Bin Ladin, who more than anyone was responsible for the September 11, 2001, terrorist attacks, is dead—killed by U.S. forces in one of the most bold and challenging counterterrorism operations in our history.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00971 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.597

At the same time, al-Qa'ida, its affiliates and adherents around the world, as well as other terrorist organizations, continue to pose a significant threat to our country. This threat is resilient and adaptive and will persist for the foreseeable future. America's campaign against terrorism did not end with the mission at Bin Ladin's compound in Abbottabad, Pakistan in May. A decade after the September 11th attacks, we remain at war with al-Qa'ida and face an evolving threat from its affiliates and adherents. Confronting this threat and working with resolve to prevent another terrorist attack is NCTC's focus, first and foremost.

In my statement, I will begin by examining the evolution of the terrorist threat. I will then describe the role of NCTC and the recent reforms we have adopted. Finally, I will identify some of the challenges we face going forward.

II. The Evolving Terrorist Threat

1. Al-Qa'ida Core and its Allies in Pakistan Pose Threat Despite Degradation

Counterterrorism successes and sustained pressure have left al-Qa'ida at its weakest point in the last ten years, and significantly degraded the group's ability to conduct attacks outside of South Asia. This is exemplified by the lack of a successful operation in the West since the 7 July 2005 transportation bombings in London. Further, the killing of Usama bin Ladin in May and last month's killing of al-Qa'ida's newest deputy, Atiyah abd al Rahman, mark strategic milestones in our fight against al-Qa'ida, and are likely to accelerate al-Qa'ida's decline, but does not mute the impact of its narrative.

Al-Qa'ida Core. Al-Qa'ida core's capability to recruit, train, and deploy operatives for anti-Western attacks has been reduced. Yet the group remains the ideological leader of the global extremist movement and continues to influence extremists through public media statements. Core al-Qa'ida's advancement of several unsuccessful smaller-scale Western plots in the past two years, including against the homeland and Europe, highlight its ability to continue some attack preparations while under sustained counterterrorism pressure, and we remain concerned al-Qa'ida may be plotting an attack against the United States at home or overseas. Moreover, while most observers view the non-violent successful tactics of the Arab Spring demonstrators in Egypt and Tunisia as a repudiation of al-Qa'ida message and approach, the group's leadership continues to seek openings for its destructive narrative. Since January they have prepared at least 12 propaganda messages related to the Arab Spring, making it a key theme of their media strategy.

- In the aftermath of Bin Ladin's death, al-Qa'ida leaders moved quickly to name his long-time deputy, Ayman al-Zawahiri, as his successor. Al-Zawahiri is the only active leader remaining from that core group of al-Qa'ida leaders who were in Afghanistan in the lead-up to 9/11. Since this announcement, some affiliates have publicly sworn allegiance and pledged support to Zawahiri, reinforcing the importance of al-Qa'ida core's leadership role in the global movement.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00972 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.598

- While al-Qa'ida core's capabilities to attack the United States are diminished, and they have failed to conduct another homeland attack in the 10 years since 9/11, the group's intent to strike us at home remains strong. In advance of the 9/11 anniversary this year, al-Qa'ida leader al-Zawahiri issued a public statement encouraging sympathizers to attack the United States.

- Recently obtained information suggests that as of February 2010, al-Qa'ida was contemplating large attacks in the homeland on symbolic dates, specifically the tenth anniversary of 9/11. However, degraded external operational capabilities suggest al-Qa'ida may seek smaller scale, achievable tactics and targets of opportunity. As of spring 2010, al-Qa'ida core believed targets worthy of the group's focus included prominent transportation, infrastructure, economic, and political targets.

Al-Qa'ida's Pakistan-Based Militant Allies. The success of Operation Enduring Freedom after 9/11 in expelling al-Qa'ida from its Afghanistan safe haven forced the group to rely on local allies and new hosts across the border in Pakistan. Since its relocation, al-Qa'ida has consistently encouraged its local militant allies to expand their operational agendas to include U.S. and Western targets—both within the region and overseas. Faisal Shahzad's May 2010 attempted bombing in Times Square is a stark reminder that al-Qa'ida allies such as Tehrik-e-Taliban Pakistan (TTP) continue to threaten U.S. interests in the Afghanistan and Pakistan region. Such threats—including threats to avenge Bin Ladin's death—have the stated intent and demonstrated capability to attempt attacks in the in the United States.

- TTP in mid-June said the group supports Ayman al-Zawahiri as al-Qa'ida's new leader and further claimed Zawahiri is TTP's "chief and supreme leader"; TTP's spokesman described al-Zawahiri as a capable person who would inspire the group to take on the West." A TTP deputy claimed in an AP interview that TTP would "complete [bin Ladin's mission] with a new zeal" and a separate leader vowed to "hit American targets outside Pakistan."

- Other al-Qa'ida allies in Pakistan and Afghanistan, notably the Afghan Taliban and the Haqqani Network, have close ties to al-Qa'ida. These groups have demonstrated the intent and capability to conduct attacks against U.S. persons and targets in Afghanistan, and we are looking closely for any indicators of attack planning in the West. Both groups also continue to provide safe haven to al-Qa'ida and neither has publicly disavowed ties to the terrorist group despite sustained counterterrorism pressure.

Lashkar-e-Tayyiba (LT)—perpetrators of the November 2008 coordinated armed assault against multiple targets in Mumbai—is one of the largest and most dangerous of the militant groups and poses a threat to a range of interests in South Asia. LT has been implicated in multiple attacks in India, including the 11 July 2006 attack on Mumbai commuter trains and the December 2001 armed assault on the Indian Parliament building. Attacks in Kashmir and India have had a destabilizing effect on the region, increasing tensions between India and Pakistan. LT is increasing its operational role in attacks against coalition forces in Afghanistan. LT has not previously conducted attacks in the United States or the West; however, LT, or individuals who trained with LT in the past but have adopted a more global extremist agenda, could pose a

threat to the homeland and the West, particularly if they were to work in collaboration with al-Qa'ida, its allies and affiliates, or other like-minded terrorists.

2. The Evolution of al-Qa'ida's Regional Affiliates and the Increasing Threat to the West

Ten years after 9/11, we face a much more diffuse and diversified threat, largely due to the emergence and evolution of regional affiliates who support al-Qa'ida core's strategy of creating a self-sustaining global extremist movement. To varying degrees, the affiliates have increased the scope of their operations, seeking to strike some U.S. and Western targets both inside and outside of their respective regions.

Al-Qa'ida in the Arabian Peninsula (AQAP). Yemen was already a key battleground and regional base of operations from which AQAP could plan attacks, train recruits, and facilitate the movement of operatives prior to the outbreak of the Arab Spring related violence earlier this year. AQAP's gains and the regime's governing challenges are increasing our concerns about the group's capability to conduct additional attacks targeting the homeland and U.S. interests overseas, as well as our concerns about the group's continuing propaganda efforts designed to inspire like-minded Western extremists to conduct attacks in their home countries.

- AQAP's two attempted attacks against the homeland—the attempted airliner attack during December 2009, and its follow-on effort to down two U.S.-bound cargo planes in October 2010 using explosives-laden printer cartridges—were indicative of a determined enemy capable of adjusting tactics to achieve success.

- AQAP also is encouraging extremists in the United States to strike here. Each of AQAP's first six issues of *Inspire* magazine has featured a section titled, "Open Source Jihad," which aims to provide easily followed instructions on weapons use, explosives construction, and targeting ideas.

Al-Qa'ida Operatives in East Africa and Al-Shabaab. East Africa remains a key operating area for the Somalia-based terrorist and insurgent group al-Shabaab and other al-Qa'ida associates. Despite recent setbacks in Mogadishu, al-Shabaab is still a significant threat to U.S. interests and remains committed to al-Qa'ida's ideology. At least 20 U.S. persons—the majority of whom are ethnic Somalis—have traveled to Somalia since 2006 to fight and train with al-Shabaab. The impact of the famine on the fighting in Somalia is not yet clear.

- In the past year, at least two young men who left the United States and traveled to Somalia were killed while fighting with al-Shabaab.

- The June death in Somalia of al-Qa'ida veteran Fazul Abdullah Muhammad, a.k.a. Harun Fazul, removes one of the most capable operatives in the region. Nonetheless, we remain concerned that foreign fighters associated with his network continue to train and plot against U.S. and Western targets.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00974 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.600

Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM). AQIM has had limited success in exploiting the Arab Spring in North Africa, and there is no indication their propaganda has found a receptive audience. AQIM threatens U.S. and other Western interests in North and West Africa, primarily through kidnap-for-ransom operations and small arms attacks; though, the group's recent execution of several French hostages and first suicide bombing attack in Niger last year demonstrate AQIM's lethality and attack range. Sustained Algerian efforts against AQIM have degraded the organization's ability to conduct high-casualty attacks in the country and compelled the group to shift its operational focus from northern Algeria to the vast, ungoverned Sahel region in the south.

- AQIM continues to hold multiple European hostages, most recently kidnapping an Italian woman in February.

Al-Qa'ida in Iraq (AQI). Ongoing counterterrorism successes against AQI—to include the deaths of the group's top two leaders last year in a joint Iraqi/U.S. military operation—have continued to put pressure on the organization. AQI's recent public statement claiming 65 separate attacks in May and June indicate the group remains an active and capable al-Qa'ida affiliate. Immediately following UBL's death the current leader of AQI publically reaffirmed his group's support for al-Qa'ida and Ayman al-Zawahiri. The arrests in May of two AQI-affiliated Kentucky-based Iraqi refugees highlight the potential threat posed by U.S.-based AQI-associates. We assess that AQI remains committed to al-Qa'ida's global agenda and are concerned they may be intent on conducting external operations, to include in the homeland.

- Al-Qa'ida in Iraq has released two Arabic-language propaganda statements encouraging individual terrorist acts, including a January video that called for lone offender attacks against Western infrastructure and students and an early April interview in which AQI's leader generally reiterated the January call for attacks and noted that weapons used in Iraq are available in most countries.

3. Homegrown Violent Extremists Activity Remains Elevated

Homegrown violent extremists (HVEs)—inspired by al-Qa'ida's global extremist agenda—are a key element of the evolution and diversification of the threat since 9/11. The growth of online English-language violent extremist content during the past three years has fostered greater cohesion, but not necessarily collaboration, among HVEs. Plots disrupted during the past year were unrelated operationally, but are indicative of a common cause rallying independent extremists to want to attack the homeland.

A key feature of this trend has been the development of a U.S.-specific narrative—a blend of al-Qa'ida inspiration, perceived victimization, and glorification of past Homegrown plotting—that addresses the unique concerns of U.S.-based violent extremists. HVEs who independently plan attacks with no direction from associates in the U.S. or overseas are difficult to detect and disrupt and could advance plotting with little or no warning.

- Arrests of HVEs in the United States in 2010 and 2011 remained at elevated levels. The arrest of U.S. Army PFC Naser Jason Abdo—who allegedly planned to kill American

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00975 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.601

soldiers near Ft. Hood—underscores our concerns about the ongoing threat from lone offender HVEs. U.S.-based extremists continue to be motivated to carry out violence on the basis of a variety of personal rationales, highlighting the continued intent by some HVEs to take part in violence despite having no operational connections to terrorists overseas.

- Al-Qa'ida core and some of its regional affiliates have repeatedly encouraged independent attacks, which could further encourage HVEs toward violent acts. Increasingly sophisticated English-language propaganda, including *Inspire* magazine, that provides extremists with guidance to carry out homeland attacks remains easily available via the Internet. English-language web forums also foster a sense of community and further indoctrinate new recruits, both of which can lead to increased levels of violent activity.

- Although al-Qa'ida's Pakistan-based senior leaders previously encouraged self-initiated attacks in propaganda, their video released on June 3rd titled, "Thou Art Held Responsible Only for Thyself," marked the group's most explicit endorsement of individual terrorist acts and first public encouragement of cyber attacks.

4. State Sponsors of Terrorism

In September 2001, seven countries—Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria—were on the State Sponsors of Terrorism List. Today, only Cuba, Iran, Sudan, and Syria remain.

Iran is still the foremost state sponsor, and since 9/11 the regime has expanded its involvement with terrorist and insurgent groups—primarily in Iraq and Afghanistan—that target U.S. and Israeli interests. Iran's Islamic Revolutionary Guard Corps-Qods Force and Ministry of Intelligence and Security have been involved in the planning and execution of terrorist acts and the provision of lethal aid—such as weapons, money, and training—to these groups, particularly Lebanese Hizballah.

- Iran's relationship with Hizballah since 9/11 has evolved from a traditional state sponsor-proxy relationship to a strategic partnership that provides a unified front against Israel and the U.S.

- During the past decade, Syria has narrowed and shifted how and who it supports as a result of such events as the 9/11 attacks, the Palestinian intifadahs, the death of Arafat, and the Iraq war. The Assad regime limits support to groups directly relevant to Syrian interests in Lebanon, the Occupied Territories, and Iraq.

- Since 2001, Sudan has taken action against several terrorist groups within Sudan and gradually improved cooperation with the U.S. and regional partners. We remain concerned about permanent improvements in Khartoum's counterterrorism legislation, HAMAS, and Palestinian Islamic Jihad remaining in Sudan.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00976 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.602

III. The National Counterterrorism Center

1. The Role of NCTC

Created in the aftermath of the attacks on 9/11, the overarching mission of the NCTC is to lead the effort to combat international terrorism. In its 2004 report, the 9/11 Commission observed that, "the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative and agile responses." That observation—as true today as it was when the 9/11 Commission issued its report—led the Commission to recommend the creation of a National Counterterrorism Center. As the 9/11 Commission proposed: "Breaking the mold of national government organization, this NCTC should be a center for joint operational planning and joint intelligence."

In December 2004, Congress established NCTC. The Intelligence Reform and Terrorism Prevention Act of 2004 set forth NCTC's key responsibilities. These responsibilities are captured in NCTC's mission statement: "Lead our nation's effort to combat terrorism at home and abroad by analyzing the threat, sharing that information with our partners, and integrating all instruments of national power to ensure unity of effort."

Intelligence Analysis and Integration. By law, NCTC serves as the primary organization in the U.S. government for analyzing and integrating all intelligence possessed or acquired by the government pertaining to terrorism and counterterrorism, except intelligence pertaining exclusively to domestic terrorism and domestic counterterrorism. NCTC has a unique responsibility to examine all international terrorism issues, spanning geographic boundaries and allowing for intelligence to be analyzed regardless of whether it is collected inside or outside the United States. NCTC has access to the entire catalogue of reporting—both foreign and domestic—on terrorism issues.

NCTC's strategic analyses are vetted and coordinated throughout the intelligence community, which adds multiple analytic perspectives. NCTC produces coordinated assessments on such critical terrorism issues as terrorist safe havens, state sponsors of terrorism, counterterrorism cooperation worldwide, and regional terrorism issues and groups. NCTC also regularly prepares intelligence assessments that are integrated into NCTC's Directorate of Strategic Operational Planning to inform policymakers on the progress of U.S. counterterrorism efforts.

NCTC's strong analytic cadre, which includes detailees and assignees from across the intelligence community, means that NCTC products reflect the diversity of the entire intelligence community and not the analytic view of one group or agency.

Watchlisting. NCTC also serves as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support. As the federal government's central and shared knowledge bank, NCTC has developed and maintains the Terrorist Identities Datamart Environment (TIDE) on known and suspected terrorists and terrorist groups. In this role, NCTC

67123.603

advances the most complete and accurate information picture to our partners to support terrorism analysts. We also support screening activities that ultimately help prevent terrorist plans and operations against U.S. interests.

Strategic Operational Planning. NCTC is charged with conducting strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities. In this role, NCTC looks beyond individual department and agency missions toward the development of a single, unified counterterrorism effort across the federal government. NCTC develops interagency counterterrorism plans to help translate high level strategies and policy direction into coordinated department and agency activities to advance the President's objectives. These plans address a variety of counterterrorism goals, including regional issues, weapons of mass destruction-terrorism, and countering violent extremism. The strategic operational planning process integrates all phases of the planning cycle—developing a plan, monitoring its implementation, and assessing its effectiveness and resource allocations—and creates communities of interest to coordinate and integrate implementation.

For example, NCTC is joining with the Department of Homeland Security and the Federal Bureau of Investigation to conduct workshops across the United States that enable cities to better develop and refine their response plans to evolving terrorist threats. These "Joint Counterterrorism Awareness Workshops" increase the ability of federal, state, local and private sectors partners to respond to a threat by discovering gaps in capabilities, planning, training and resources; and identify existing programs or resources that can close those gaps. The workshops also provide a venue to share best practices at the state and local levels and serve as a basis for identifying issues and gaps that may subsequently be addressed nationwide.

Interagency Threat Assessment and Coordination Group. In 2007, this Committee played an integral role in creating the Interagency Threat Assessment and Coordination Group, or ITACG. Located at NCTC, the ITACG is led by DHS in partnership with the FBI. The group brings together federal and nonfederal intelligence, law enforcement and first responder communities and is dedicated to bridging the intelligence information gap between traditional intelligence agencies and state, local, tribal and private sector partners. The ITACG's role in the intelligence community is to advocate for the intelligence and information needs of these key partners and to help federal intelligence agencies improve the way in which they produce and disseminate intelligence information to intelligence customers. The ITACG has representatives from a geographically diverse set organizations and agencies, with expertise in law enforcement, fire and rescue, and health services.

2. Key NCTC Initiatives

With the support of Congress, NCTC and the rest of the government have made strides in the fight against terrorism, but much work remains. We face threats from a dynamic and complex terrorist environment. NCTC is committed to changing and adapting to meet these threats and the challenges they present. In particular, over the last two years—with lessons learned from the failed airline bombing in December 2009—NCTC has implemented several initiatives to improve our ability to identify and prevent terrorist attacks.

Pursuit Group. In January 2010, NCTC created the Pursuit Group to develop tactical leads and pursue terrorism threats. The formation of the Pursuit Group has provided the counterterrorism community with a group of co-located analysts that have unparalleled data access and expertise, which enables Pursuit Group to focus exclusively on information that could lead to the discovery of threats aimed against the homeland or U.S. interests abroad. With teams comprised of personnel from across the intelligence community, with access to the broadest range of terrorism information available, Pursuit Group analysts are able to identify actionable leads that could otherwise remain disconnected or unknown. While the majority of the intelligence community understandably follows current threats, Pursuit Group analysts can ensure that terrorism cases are examined as thoroughly as possible by pursuing non-obvious and unresolved connections, identifying unknown, known or suspected terrorists, and focusing on seemingly unimportant details that could yield relevant information.

The Pursuit Group provides investigative leads, collection requirements, and potential source candidates to operational elements like the FBI, CIA, or DHS for intelligence purposes or action. During the first 3 quarters of Fiscal Year 2011, the Pursuit Group completed over 800 actions that provided the counterterrorism partners, including the federal law enforcement community, with new knowledge and analysis on tactical terrorism threats. These actions range from communicating directly with other agencies via cable to providing information for TIDE, watchlisting, and no-fly nominations.

Watchlisting and TIDE. NCTC has adopted important reforms in the watchlisting process and has improved NCTC's receipt, processing, and the quality of information sharing in support of the Center's watchlisting and screening responsibilities. Specifically, the intelligence community adjusted the minimum identifying information necessary to allow additional individuals to be entered into the Terrorist Identities Datamart Environment (TIDE) and took other measures to ensure more effective record and database searches, correlation of data, and processing of encounters. In July 2010, the community watchlisting guidance was revised to provide flexibility to push forward information that previously had not met the requirements. The added features include a bulk ingest application, automatic processing of the nominations, and exporting records to the Terrorist Screening Center in near-real time. We also increased our ability to store, compare, match, and export biometrics such as fingerprint, facial images, and iris scans. At the same time, however, we have taken great care to ensure that our core civil liberties and privacy protections are preserved. Nominations of U.S. persons to a watchlist must still be supported by "reasonable suspicion" that the person is a "known or suspected terrorist," and a person cannot be watchlisted based solely upon First Amendment protected activity, or based solely upon race, ethnicity, or religious affiliation.

One of the key gaps we identified in the watchlisting process was the need to enhance existing TIDE records with additional information. NCTC is now taking a more aggressive and innovative approach to seek methodologies and data repositories to ingest biographic, biometric, and derogatory information. We also are conducting large scale data correlation efforts on a nightly basis, enabling discovery of previously unknown terrorist connections and attributes. As the threat continues to evolve, our watchlisting experts are proactively partnering with NCTC's Pursuit Group and the counterterrorism community to expedite the sharing of information to build more complete terrorist identities.

Information Technology. NCTC has implemented several significant improvements to its information technology. These include:

- expanding advanced data correlation services to process and filter massive data sets;
- improving technology supporting the development of leads to identify non watchlisted names or aliases; and
- updating NCTC's integrated data repository with several country-specific data sets.

For example, prior to December 2009, analysts were required manually to search and integrate information—data from multiple networks residing in specific databases had to be searched, selected, and copy/pasted to get the relevant information to the analyst's primary workspace. Now, NCTC's "Counterterrorism Data Layer" is being developed to ingest relevant data and to allow NCTC analysts to search, exploit, and correlate terrorism information in a single environment. Thanks to the efforts of the DNI, Secretary Napolitano, Director Mueller, and the Directors of the CIA, NSA, and DIA, NCTC is acquiring priority data sets for ingestion, and for the first time, NCTC analysts can search across key homeland security and intelligence information and get back a single list of relevant results. Moreover, sophisticated analytical tools are in place to permit analysts to conduct 'Google-like" searches, conduct link analysis and data visualization, and to triage information. These efforts are being pursued with careful consideration of legal, policy, and technical issues to protect privacy and civil liberties.

Countering Violent Extremism. Over the past ten years, the government has expanded its counterterrorism efforts to include a focus on preventing al-Qa'ida and its adherents from recruiting and radicalizing the next generation of terrorists, both overseas and at home. Efforts to prevent and counter violent extremism focus on undercutting the terrorist narrative, improving government and law enforcement expertise for understanding the threat, and building more resilient communities—making radicalization and recruitment to violence more difficult for al-Qa'ida's and its allies and affiliates. Because this new approach takes a more holistic view of the threat, it requires the active engagement of departments and agencies whose missions go beyond traditional counterterrorism and law enforcement missions.

In this framework, the National Security Council (NSC) is leading a "whole of government" approach for the U.S. Government's efforts to counter violent radicalization, as described in the August 2011 domestic radicalization strategy, *Empowering Local Partners to Prevent Violent Extremism in the United States*. NCTC supports the NSC implementation of the strategy by working closely with our federal partners, as well as with state, local and tribal partners to build and support programs, activities, and efforts that directly and indirectly counter violent extremism.

NCTC Workforce. As NCTC re-doubles its efforts to meet the challenges posed by al-Qa'ida, its affiliates and adherents, our progress is dependent on our dedicated and diverse workforce. The talented men and women who work at NCTC perform a unique and vital service to the nation, NCTC has benefitted from the integration of analysts and planners from across the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00980 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.606

intelligence community, the U.S. military, and other federal, state, and local partners. Maintaining this diversity through continued commitment from intelligence agencies and other organizations is a priority for NCTC. We continue to strengthen this workforce by providing the training, resources, and leadership needed to ensure the Center's continued success.

IV. Challenges Ahead

We continue to address challenges in dealing with the dynamic and adaptive terrorist threat environment. The nature of the threat challenges our analysts' ability to sort and connect critical bits of information across disparate data sets. The rapid change and proliferation in communications technologies require a proactively postured intelligence community, while effectively balancing the protection of sources and methods, and the need to share information.

The drawdown of U.S. military forces in Iraq and changes in relationships with key partners, such as Egypt, may affect our ability to maintain access to long-term targets. The potential impacts of the Arab Spring and upheaval in the Middle East are not yet fully understood, particularly as they relate to the al-Qa'ida narrative and key relationships.

While remaining vigilant against foreign-inspired threats, efforts to build resilience within our communities are essential to continuing progress against al-Qa'ida inspired radicalization recruitment, and mobilization to violence here at home. Engagement and partnerships with communities remain important to protecting them from the influence of al-Qa'ida, its affiliates and adherents. Integrating and harmonizing the efforts of federal, state, local, and tribal entities will remain a challenge—one we must continue to pursue.

Finally, all of our efforts must be consistent with our core values. We must carry out the mission of NCTC in a manner that retains the trust of the American people and remains true to the oaths we have taken to support and defend the Constitution. NCTC is committed to fulfilling this solemn responsibility by protecting civil liberties and privacy and respecting the rule of law. While we work to protect the Nation, we are dedicated to upholding the trust of the American people and exemplifying the values on which the nation was founded.

* * *

Chairman Lieberman, Ranking Member Collins and members of the Committee, I thank you for the opportunity to testify before the committee today. Your support has made it possible to reduce the likelihood of a successful terrorist attack. As you know, perfection is no more possible in counterterrorism than it is in any other endeavor. NCTC, in partnership with the entire counterterrorism community, continues to work tirelessly to reduce the likelihood of an attack, but we cannot guarantee safety. We must continue to foster the resilience of the American people to prepare for a potential attack.

With your determined leadership, NCTC and our key partners—sitting here with me today—we have established a strong posture against the enemies who seek to do us harm, and will continue to make progress in this fight. Every day, the threat information we review underscores the fluid and dynamic terrorist threat to the United States. We must work relentlessly to reduce that threat to our nation. In the months and years to come, I look forward to working with this Committee and the rest of Congress to keep the American people safe.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00981 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.607

OFFICERS OF THE NATIONAL COMMISSION
NATIONAL CHAIR
ROBERT G. SUGARMAN
NATIONAL DIRECTOR
ABRAHAM H. FOXMAN
PAST NATIONAL CHAIRS
BARBARA B. BALSER
HOWARD P. BERKOWITZ
KENNETH J. BIALKIN
BURTON M. JOSEPH
BURTON S. LEVINSON
GLEN S. LEWY
MELVIN SALBERG
DAVID H. STRASSLER
GLEN A. TOBIAS
VICE CHAIRS
MEYER EISENBERG
JAMES GROSFELD
THOMAS C. HOMBURGER
CYNTHIA MARKS
RUTH MOSS
PAM SCHARLER
JOSEPH SMUKLER
GEORGE STARK
GERALD STEMPLER
MYRON ZIMMERMAN
HONORARY VICE CHAIRS
RUDY BOSCHWITZ
EDGAR M. BRONFMAN
LEO GREENLAND
IRWIN HOCHBERG
GERI M. JOSEPH
MAX M. KAMPELMAN
BERNARD MARCUS
SAMUEL H. MILLER
MILTON MOLLEN
LESTER POLLACK
ALVIN J. ROCKOFF
ROWLAND SCHAEFER
TREASURER
ROBERT H. NAFTALY
ASSISTANT TREASURER
MURRAY KOPPELMAN
SECRETARY
I. BARRY MEHLER
ASSISTANT SECRETARY
STANFORD BARATZ
STANDING COMMITTEE CHAIRS
ADMINISTRATION
CHARLES F. KRISER
AUDIT
ROBERT H. NAFTALY
BUDGET
LAWRENCE ROSENBLOOM
CIVIL RIGHTS
HOWARD W. GOLDSTEIN
DEVELOPMENT
BARRY CURTISS-LUSHER
EDUCATION
RICHARD D. BARTON
INFORMATION TECHNOLOGY
JOSEPH A. GOLDBLUM
INTERNATIONAL AFFAIRS
DAVID J. MILLSTONE
LEADERSHIP
PAMELA SCHWARTZ
LEGACY/FUNDING FOR THE FUTURE
CHRISTOPHER WOLF
MARKETING & COMMUNICATIONS
MICHAEL J. RUBINSTEIN
OUTREACH & INTERFAITH AFFAIRS
MARTIN L. BUDD
PLANNING
MARVIN D. NATHAN
REGIONAL OPERATIONS
LAWRENCE J. MILLER
WASHINGTON AFFAIRS
KENNETH M. JARIN
DEPUTY NATIONAL DIRECTOR
KENNETH JACOBSON
DIVISION DIRECTORS
CIVIL RIGHTS
DEBORAH M. LAUTER
DEVELOPMENT
CLIFFORD SCHECHTER
EDUCATION
DAVID S. WAREN
FINANCE AND ADMINISTRATION
MICHAEL A. KELLMAN
INFORMATION TECHNOLOGY
SAM MEMBERG
INTERNATIONAL AFFAIRS
MICHAEL A. SALBERG
LEADERSHIP
MARVIN S. RAPPAPORT
MARKETING & COMMUNICATIONS
HOWARD A. ZAR
REGIONAL OPERATIONS
ROBERT WOLFSON
WASHINGTON AFFAIRS
STACY BURDETT
GENERAL COUNSEL
LENORE R. KREITMAN

September 14, 2011

The Honorable Joseph I. Lieberman
Chair
Senate Committee on Homeland Security and Government Affairs
United States Senate
Washington, DC 20510

The Honorable Susan Collins
Ranking Member
Senate Committee on Homeland Security and Government Affairs
United States Senate
Washington, DC 20510

Dear Chairman Lieberman and Ranking Member Collins:

Following the Senate Committee on Homeland Security and Government Affairs September 13 hearings, "Ten Years After 9/11: Are We Safer?" we write to provide the Committee with the views of the Anti-Defamation League on several aspects of this issue. We would ask that this statement be made part of the formal hearing record.

In the ten years since the September 11 terrorist attacks, our nation has experienced a number of changes that have affected our domestic and foreign policies, our sense of security, and our identity as a nation.

One way the Anti-Defamation League is commemorating the tenth anniversary is by publishing a new report, *9/11 Ten Years Later: The Changing Face of Hate, Terrorism and Democracy in America*. The report is an assessment on a range of issues that came into focus in the aftermath of the attacks, including the threat of homegrown extremism, the spread of anti-Semitic conspiracy theories, the rise of anti-Muslim bigotry, and the recalibration of the balance between security and individual rights.

The full report is available at the ADL Web site: http://www.adl.org/911-ten-years-later/pdf/911-retrospective.pdf

We have attached excerpts from our report, including the most relevant sections for this specific Committee hearing:

- Post-9/11 Islamic Extremism in the U.S. A growing number of American citizens and residents motivated by ideologies of extreme intolerance have been involved in terrorist plots.

- Muslim Extremists Targeting Jews after 9/11. Since the 9/11 attacks, a significant number of terror plots in the U.S. have targeted Jewish institutions or were fueled by hatred of Jews and Israel.

ANTI-DEFAMATION LEAGUE, 605 THIRD AVENUE, NEW YORK, NY 10158-3560 212-885-7700 FAX: 212-867-0779 WWW.ADL.ORG

- Homegrown Extremism after 9/11. Domestic terrorism remains a substantial threat, not just from domestic Muslim extremists but from white supremacists and anti-government extremists as well.

- Recalibrating the Balance between National Security and Civil Liberties. While our government focuses on preventing terrorism and extremism on American soil, the protection of our civil liberties remains crucial.

Please do not hesitate to contact our office if you have questions about these materials or if we can be of assistance to you in any way.

Sincerely,

Michael Lieberman
Washington Counsel

Stacy Burdett
Washington Director

67123.609

Post-9/11 Islamic Extremism in the U.S.

Introduction

The ideologies of extreme intolerance that motivated the 19 hijackers responsible for carrying out the September 11, 2001, terrorist attacks continue to pose a serious threat to the U.S.

While no attacks of that magnitude have been successful on American soil in the ten years since 9/11, one of the most striking elements of today's terror threat picture is the role that a growing number of American citizens and residents motivated by radical interpretations of Islam have played in criminal plots to attack Americans in the United States and abroad.

Although they do not constitute a fully coherent movement in the U.S., more and more American citizens and residents are being influenced by ideologies that justify and sanction violence commonly propagated by Islamic terrorist movements overseas.

In addition to disagreements with perceived American actions against Muslims around the world, these extremists believe that the West (and America specifically) is at war with Islam and it is the duty of Muslims to defend the global Muslim community through violent means. They come from diverse backgrounds and, as a whole, do not easily fit a specific profile. About one fourth are converts to Islam who embrace the most extreme interpretations of the religion.

The most common targets in the U.S. have been military installations, major landmarks, transit systems and Jewish or Israeli institutions. In fact, hatred of Jews and Israel has played an alarming role in the radicalization process of many of these same homegrown extremists.

Although most individuals or groups lack the means and materials to carry out violent attacks – plots have been foiled by law enforcement at various stages – they continue to demonstrate a willingness to conduct attacks in the U.S.

Influenced by Terrorists Overseas

The past three years have been marked by an increase in the number of plots and conspiracies by homegrown Muslim extremists, as well as in the number of Americans attempting to travel abroad to train and fight with terrorist groups. The latter raises serious concerns about extremists using their American passports to return to the U.S. in order to carry out attacks on U.S. soil.

Indeed, the failed attempt to bomb New York's Times Square in 2010, as well as the foiled plot to detonate homemade explosives on New York City subways in 2009, were conceived by Americans who received training from terrorist groups overseas before

67123.610

returning to the U.S. to carry out the attacks.

Approximately 30 U.S. residents have attempted to or successfully traveled to Somalia to join Al Shabaab, an Al Qaeda-linked terrorist group, since 2007 to receive weapons training alongside recruits from other countries. Several others have provided material support for the group through their recruitment and fundraising efforts.

A 27-year-old recruit from Minneapolis, Farah Mohamad Beledi, was one of two suicide bombers who attacked a military base in the Somali capital Mogadishu on May 30, 2011, according to the FBI. A portion of the Al Shabaab audio statement claiming responsibility for the attack featured Beledi saying, "I have been a member of Al Shabaab for two years. I am from Minnesota, USA," and "I am so happy to turn my body into shrapnel for the infidels." Beledi is the second confirmed American suicide bomber. The first, Shirwa Ahmed, carried out a suicide bombing on behalf of Al Shabaab at the Ethiopian Consulate and the presidential palace in Hargeisa killing 24 people in October 2009.

Foreign terrorist organizations have also appealed to Western audiences through English-language propaganda distributed on a variety of online platforms, including materials specifically designed to recruit followers and sanction violence.

The ability of foreign terrorist groups to motivate Americans to join their cause is not limited to the Internet or to Al Qaeda-affiliated groups producing propaganda targeting westerners. For example, David Coleman Headley, of Chicago, pleaded guilty to helping plan a number of terrorist attacks, including a series of coordinated attacks in November 2008 that killed more than 170 people in Mumbai. Headley conducted reconnaissance of a number of the targeted locations for Lashkar-e-Taiba (LET), the Pakistani-based Islamic terrorist organization. Several other American citizens have been charged with providing material support to LET.

Online Propaganda Encourages Terror

Many American extremists have been influenced by English-language terrorist propaganda and recruitment materials on Web sites, forums, blogs, social networking sites, video-hosting sites and other online platforms. These materials are filled with colloquial Western references and practical advice designed specifically for an American audience.

Omar Hammami, an Alabama native who has become the public face and voice of Al Shabaab, has appeared in several videos urging foreigners "to come and live the life of a mujahid." In a March 2009 video, Hammami praised a killed fighter as a martyr and said, "We need more like him, so if you can encourage more of your children and more of your neighbors and anyone around you to send people like him to this jihad, it would be a great asset for us."

In addition, the media wing of Al Qaeda in the Arabian Peninsula (AQAP), Al Qaeda's affiliate in Yemen and Saudi Arabia, has deliberately designed a portion of its propaganda to appeal to, engage and recruit sympathizers in the U.S. Since July 2010, AQAP has released several issues of its online English-language magazine *Inspire*, which employs accessible Western references and colorful graphics in its calls to inflict mass casualties. AQAP, which has instructed readers to "fight jihad on U.S. soil," encourages participation in the production of the magazine, asking readers to contribute articles, quotes and images.

One recurring section in *Inspire*, entitled "Open Source Jihad," provides a resource manual for "Muslims to train at home instead of risking a dangerous travel abroad" and

67123.611

proposes several ways to wage "individual jihad" that inflicts mass casualties and economic losses. "We strongly encourage our brothers to fight jihad on U.S. soil," the author writes. "To kill a snake, strike its head." The October 2010 issue included a picture of the Chicago skyline, perhaps foreshadowing the terror plot against Chicago-area synagogues on October 29, for which AQAP claimed responsibility.

Mohamed Osman Mohamud, who was arrested in November 2010 for attempting to blow up a Christmas tree lighting with a car bomb in Portland, Oregon, submitted an article to *Inspire* (it was not published) as well as to another English language online terror magazine called *Jihad Recollections*.

Influence of Anwar al-Awlaki

Anwar al-Awlaki is among a growing chorus of Americans residing abroad who use their online pulpits to reach and influence audiences in the U.S. by repackaging ideologies of extreme intolerance and violence into digestible sound bites.

One indication of al-Awlaki's widespread influence is the number of extremists that have been found in possession of his materials. The list includes many of those arrested in 2010, among them Antonio Martinez, a Maryland man arrested for attempting to detonate what he believed to be a car bomb at a Maryland army recruiting center in December; Ahmed Farooque, a Virginia man who was arrested in October for allegedly plotting attacks against Metro stations in the Washington Metropolitan Area and Barry Walter Bujol, Jr., a Texas resident arrested for attempting to deliver money and other equipment to AQAP.

Anwar al-Awlaki's mass appeal has also resulted in his taking a public role with Al Qaeda in the Arabian Peninsula (AQAP), Al Qaeda's affiliate in Yemen and Saudi Arabia that has deliberately designed a portion of its propaganda to appeal to, engage and recruit sympathizers in the U.S.

Many others have been influenced by al-Awlaki as well, most notably Nidal Malik Hasan, who allegedly killed 13 people at the Fort Hood army base after exchanging emails with al-Awlaki. The shooting at Fort Hood followed a separate incident in June 2009 when Abdulhakim Mujahid Muhammad allegedly shot two uniformed American soldiers, killing one of them, at a military recruiting center in Arkansas.

While most of the plots in the U.S. have been foiled by law enforcement before they were carried out, the Fort Hood and Arkansas attacks demonstrate the particular danger posed by so-called "lone wolf" extremists who, though unaffiliated with terrorist groups, share their radical interpretations of Islam and ideological goals.

67123.612

ADL's Role in Fighting Islamic Extremism

As part of its ongoing effort to combat Islamic extremism, ADL has:

- Issued reports detailing the growing and increasingly dangerous domestic terror threat posed by American Muslim extremists, which has been very helpful to law enforcement as well as Congress in hearings held to assess current threats.
- Shared analysis and resources with Rep. Peter T. King (R-NY), Chairman of the House Committee on Homeland Security, and other committee members on how homegrown extremists are influenced by terrorist propaganda and recruitment materials on various online platforms.
- Distributed *Terrorism Update,* an online publication that details trends in domestic terrorism.
- Provided training to law enforcement officers around the country.
- Shared actionable intelligence with law enforcement agencies.
- Assisted in an FBI investigation into Zachary Adam Chesser, arrested in July for providing material support to an Al Qaeda-linked terrorist group, communicating threats and seeking to incite crimes of violence. ADL had been tracking Chesser's extensive online activity since 2009.
- Received commendation from FBI Director for assistance in preventing a terrorist plot to blow up a courthouse.
- Cited by national and international media, including *The New York Times, Washington Post, Wall Street Journal, Los Angeles Times, Chicago Tribune*, CNN, FOX News, ABC News and the BBC.
- Provided the Library of Congress's Congressional Research Service extensive information for its report, "American Jihadist Terrorism: Combating a Complex Threat," released in September 2010.

67123.613

Muslim Extremists Targeting Jews After 9/11

Introduction

The terrorists responsible for the September 11, 2001, attacks were motivated, in part, by an ideology rooted in the hatred of Jews. Mohamed Atta, a key member of the Al Qaeda Hamburg cell responsible for the attacks, considered New York City to be the center of a global Jewish conspiracy, and Khalid Sheik Mohammed, who masterminded the attack, had previously developed several plans to attack Israeli and Jewish targets. In their view, New York, as a center of world finance, was the quintessential Jewish target.

In the years since the attacks, a significant number of American citizens and residents involved in terror plots in the U.S. have been influenced by violent ideologies developed by Al Qaeda and other foreign terrorist organizations that promote hatred of Jews and Israel.

According to these ideologies, Jews are the eternal enemy of Muslims and the embodiment of true evil. Al Qaeda-affiliated extremists and those who have adopted a similar ideology have long referred to their enemies as "Zionist-Crusaders," the "Jewish-Crusader Alliance," or the "Jews and Crusaders," thereby identifying Jews as a key component of the forces they view being at war with Islam.

Al Qaeda's ideology, which was developed by the original ideologues of Islamist terrorism, led to attacks against distinctly Jewish targets around the world beginning in 2002. Since then, these anti-Jewish themes have increasingly been propagated online, including in English-language terror propaganda intended to reach and appeal to Western audiences.

As a result, American citizens and residents influenced by these ideologies of extreme intolerance have not only expressed hatred of Jews and Israel, but also in several cases specifically targeted Jewish institutions.

While most plots in the U.S. since 9/11 have been foiled by law enforcement before they were carried out, several cases demonstrate the willingness, if not the capacity, of extremists motivated by radical interpretations of Islam to target Jews.

Plots against the New York Jewish Community

Several post-9/11 plots and conspiracies targetting Jews have taken place in New York. For example, in May 2011, Ahmed Ferhani, a legal resident from Algeria, and Mohammad Mamdouh, a naturalized U.S. citizen of Moroccan decent, were arrested for plotting to attack a synagogue in New York City in order to advance their radical ideological goals. New York Police Commissioner Raymond Kelly said Ferhani, who attempted to purchase weapons, including guns and a hand grenade, planned to grow out his beard in order to look "more like a Jew" and enter a synagogue more easily.

A similar plot occurred in 2009, when four men, including three American Muslim converts, planned to attack synagogues in the Bronx and a military base in Newburgh, in

67123.614

response to perceived American actions against Muslims around the world. The men planted what they believed to be bombs in cars outside of the Riverdale Temple and the nearby Riverdale Jewish Center. In a conversation with an undercover informant, one of the plotters, James Cromitie stated his desire to "destroy" the Jews. "The worst brother in the whole Islamic world is better than 10 billion Yahudi (Jews)," Cromitie stated. "With no hesitation, I will kill 10 Yahudis."

In 2007, Russell Defreitas, a naturalized U.S. citizen from Guyana, and three other men, were arrested for plotting to attack New York's John F. Kennedy International Airport. The men planned the attack in part because they wanted to take revenge on the U.S. for its diplomatic relationship with Israel. Defreitas later told an informant that Muslims "incur the wrath of the world while Jews get a pass," and that he "wanted to do something to get those bastards." Court documents have also alleged that Defreitas had suggested targeting a nearby Jewish school or a predominately Jewish neighborhood.

Post-9/11 plots targeting Jews have occurred outside of New York as well, including a 2005 plot in Los Angeles to attack military and Jewish targets, including synagogues and the Israeli Consulate, and a 2002 plot targeting Jewish institutions and other targets in Southern Florida.

Hatred of Jews and Israel a Motivating Factor

Several plots, while not directly targeting Jewish institutions, have been motivated in part by hatred of Jews and Israel. For example, in 2007, Mohamad Ibrahim Shnewer, a naturalized U.S. citizen, and four other Muslim immigrants conspired to kill American soldiers at New Jersey's Fort Dix army base. According to court documents, "anti-Zionist hatred is one of the reasons, if not the primary reason why they planned to attack Ft. Dix." The Department of Justice further alleged that the men were motivated by "their desire to 'avenge' the supposed crimes of Zionism." Shnewer told an undercover informant that his first choice was to kill Jews in Israel: "I love to kill Jews. I tell you this, in all honesty, it is a dream of mine."

Hatred of Jews and Israel has also influenced deadly attacks carried out by "lone wolf" Muslim extremists. Nidal Malik Hasan, an Army psychiatrist from Virginia who killed 13 people at the Fort Hood Army base in Texas, expressed his support of killing Jews and Israelis in a series of e-mails exchanged prior to the attack with Anwar al-Awlaki, an American Muslim cleric living in Yemen who has influenced several extremists through his English-language propaganda and recruitment materials online.

The shooting at Fort Hood followed a separate incident in June 2009 when Abdulhakim Mujahid Muhammad shot two uniformed American soldiers, killing one of them, at a military recruiting center in Arkansas. Muhammad, an American Muslim convert, reportedly searched for information about Jewish institutions on the Internet. After his arrest, Muhammad admitted to throwing a fire bomb at the house of an Orthodox Rabbi in Nashville, Tennessee, and confessed to firing shots at the home of Little Rock rabbi in the days before his attack on the recruiting center.

Although post-9/11 plots and conspiracies in the U.S. are increasingly led by or involve American Muslim extremists, the threat from foreign nationals remains. In September 2009, for example, Hosam Maher Husein Smadi, of Jordan, attempted to detonate what he believed were explosives at the 60-story Fountain Place building in Dallas, Texas. In addition to expressed his desire to attack the U.S. for its incursions in Iraq and Afghanistan, Smadi also espoused a hatred of Israel and Jews, calling for the "destruction of the Jews."

67123.615

Spreading the Message Online

Calls for attacks against Israel and Jews are often included in the English-language terrorist propaganda created by foreign terrorist organizations and disseminated online to reach and appeal to Western audiences. For example, in the first pages of the October 2010 issue of Al Qaeda in the Arabian Peninsula's *Inspire* magazine, the editor warns that they will "not lay down their arms until they free this land from the tyrants and march on to Jerusalem. That is when America and its Jewish masters would realize the true danger of AQAP."

In November 2010, AQAP claimed responsibility for a mail bomb plot involving Chicago-area Jewish institutions. The AQAP statement, which threatened additional attacks against American interests, also vilified Saudi Arabia for their alleged cooperation with the Jews and for providing intelligence that enabled Western officials to locate and diffuse the explosive-laden packages. "Allah has exposed your true servitude to the Jews, for these devices were heading towards Zionist Jewish synagogues, but you interfered with your known treachery to protect them."

According to AQAP, the packages were addressed to the synagogues "in Chicago, Obama's city," because AQAP is "facing a coalition of Crusaders and Zionists" and "will never forget Palestine."

As anti-Semitism continues to be intrinsic to the ideology of foreign terrorist organizations and their adherents in the U.S., the American Jewish community must remain vigilant.

ADL Takes Lead in Protecting the Jewish Community

As part of its ongoing effort to protect Jewish communities against the threat posed by Muslim extremists, ADL has:

- Issued reports detailing the growing and increasingly dangerous domestic terror threat posed by Muslim extremists, which has been very helpful to law enforcement as well as Congress in hearings held to assess current threats.
- Provided training to law enforcement officers around the country.
- Shared actionable intelligence with law enforcement agencies.
- Provided actionable intelligence, practical security alerts and clear security guidance to the Jewish community.
- Developed and deployed sophisticated security materials and training, including the comprehensive *Protecting your Jewish Institution,* the only Jewish communal specific manual dealing with security.
- Delivered dozens of security briefings and messages each year to the community via our on-the-ground network of regional offices.

67123.616

Homegrown Extremism after 9/11

Introduction

In the ten years since the September 11 terrorist attacks, international terrorist organizations have frequently attempted sequels to the events of that day. No such attempts on American soil have succeeded, a testament to America's law enforcement agencies and intelligence services and to those of its allies. International terrorism, however, still remains the biggest potential threat to American security.

Though law enforcement and intelligence agencies have prevented any further attacks similar to 9/11 on American soil, the United States has not been free from terrorism. On the contrary, this country has seen a series of such acts, ranging from bombings to targeted killings to arsons, as well as an even greater number of ultimately unsuccessful conspiracies and plots. These violent incidents have been carried out not by international terrorists but by adherents of homegrown or domestic extremist movements. Such movements have historically been the main sources of terrorism in the United States and remain so today.

While the United States must remain vigilant against the threat of international terrorism and devote significant resources to that problem, it must understand, too, that homegrown terrorism will always remain a substantial and consistent threat. Fortunately, many of the reforms and programs implemented after 9/11 to combat international terror threats have aided in the fight against domestic extremist criminal activity, as well.

Sources of Violence

With a population of over 310 million people, the United States has a number of fringe ideological, religious and social movements whose followers may be motivated to take violent action. During the past ten years, four extreme movements have contributed the most to domestic terrorism and criminal extremism:

- **White Supremacists.** The oldest source of domestic terrorism in the United States, white supremacists remain one of its mostly deadly, with adherents committing violent crimes ranging from hate crimes to major terrorist plots. At the time of the 9/11 attacks, white supremacist movements had receded from a six-year resurgence in the mid-to-late 1990s that had resulted in a spate of terrorist acts and conspiracies. During the 2000s, white supremacist terrorist acts tended to be narrower in focus and smaller in scope, such as pipe-bombs and letter-bombs. From 2008 onwards, however, white supremacists have experienced a resurgence that, while not matching its 1990s counterpart, has nevertheless resulted in increased acts of violence, especially shootings.

- **Anti-Government Extremists.** Even more so than white supremacists, anti-government extremists (especially the militia and sovereign citizen movements) have experienced a major uptick in both activity and numbers since 2008, a resurgence that has caused problems across the country, including lethal shootings and major plots to kill law enforcement officers and judges. The sovereign citizen movement, which does not acknowledge the legitimacy or authority of the government at all, has experienced the most growth and is

67123.617

causing the most problems in 2011.

- **Domestic Muslim Extremists.** In the past decade, domestic Muslim extremists have emerged as a significant terror threat, engaging in a number of major conspiracies and several lethal shooting incidents. As a movement, they are not fully formed, responding more to external influences (such as Yemen-based cleric Anwar Al-Awlaki) than to homegrown ones. They also constitute a textbook example of what terrorism analysts describe as a "high intent, low capability" threat. Most conspiracies emerging from this movement over the past decade were uncovered and broken up by law enforcement, often through "sting" operations, long before they could be carried out to fruition. However, were the movement's tactics to change, it could become more deadly.

- **Environmental/Animal Rights Extremists.** The extreme wings of the broader environmental and animal rights movements have perpetrated many violent acts during the 2000s, primarily through fire-bombings and arsons, some of which have caused millions of dollars of damage. Such was the frequency of the attacks—and the inability of law enforcement to find their perpetrators—that the FBI in 2005 declared them the nation's top domestic terror threat. Adherents traditionally abstained from attacking people, as opposed to property, rendering them less dangerous than the other extremist movements discussed here. Increasingly, however, scientists and others perceived as responsible for the mistreatment of animals or the environment are viewed by the movement as legitimate targets. Recent campaigns have been marked by militant rhetoric and, at times, acts of intimidation and violence deliberately targeting individuals. Nevertheless, major attacks are infrequent, no one has yet been seriously harmed as a result of crimes carried out in the name of animal and environmental protection, and investigations by authorities have led to a number of significant arrests and incarcerations in recent years.

The Toll of Extremism

In the decade since the 9/11 attacks, homegrown extremists have committed thousands of violent crimes, from sabotage and property destruction to hate crimes to shootings to terrorist plots and conspiracies. Many extreme movements also routinely engage in other criminal activities, such as frauds and scams or the acquisition of illegal weapons.

One way to examine the problem is to look at the most extreme results: killings that can be attributed to homegrown extremists. The true number of such deaths will never be known, as extremist connections in criminal cases sometimes take years to emerge, if at all, but there have been at least 201 deaths in the United States since 9/11 that can reasonably be associated with domestic extremists.

The breakdown (see chart) may be surprising: an overwhelming number of deaths (84%) can be attributed to just one source: white supremacists. Domestic Muslim extremists come in a distant second at 7%, but 13 of the 14 deaths in this category came from a single incident: the deadly 2009 shooting spree at Fort Hood by Nidal Malik Hasan. Anti-government extremists are third with 6% of the total—however, their killings are more targeted, including more than a third of the murders of law enforcement officers killed by extremists during this period. The total also takes into account a few isolated deaths associated with left-wing extremism or anarchism, anti-immigration extremism, and anti-abortion extremism.

Two related issues are worth pointing out. First a number of the killings by white supremacists involved traditional criminal motives rather than ideological ones.Overall, only about 49% of the killings were clearly related to a perpetrator's ideology or to

67123.61B

extremist group concerns (such as killing suspected informants). Another 42% were non-ideological or purely criminal in nature, from murdering relatives to killing police officers while in the commission of a non-ideological crime. In about 9% of the killings, the perpetrators seemed to have mixed motives or their motives were not easily identifiable. White supremacists were by far the source most likely to engage in non-ideological killings, both because many white supremacists also engage in traditional criminal activity and because white supremacist movements tend to attract many people with basic violent tendencies.

Second, homegrown extremists tend to be most dangerous when working alone as so-called "lone wolves." In general, extremists who acted in groups or cells when planning terrorist acts were caught before they could actually commit the acts. In contrast, extremists working alone, choosing more realistic targets and more obtainable weapons (guns rather than rocket launchers, for example), were far more likely to succeed in causing injury or death. This has held true for white supremacists, anti-government extremists and domestic Muslim extremists alike.

Just as the United States will continue to confront a variety of threats from international terrorists in the coming years, so too will it face the threat of violence from a variety of homegrown extremists who are already in the country in great numbers.

ADL: Responding to the Homegrown Terror Threat

As part of its ongoing effort to respond to the threat of homegrown terrorism, ADL has:

- Issued dozens of reports alerting the public and authorities to emerging domestic extremist-related threats. Also created a basic instructional guide: *The Guidebook on Extremism for Law Enforcement* (second edition now in preparation).

- Sent out monthly regional intelligence bulletins to thousands of law enforcement officers across the country to provide them with the latest intelligence on extremist-related incidents, events, and trends.

- Trained over 75,000 federal, state and local law enforcement officers on subjects related to homegrown extremist movements.

67123.619

Recalibrating the Balance between National Security and Individual Rights

Introduction

In the immediate aftermath of the September 11 terrorist attacks, our leaders in Washington quickly focused on efforts to apprehend and punish those responsible for the attacks – and to prevent future attacks on the United States and its citizens. This led to a serious national debate over, and recalibration of, the balance between civil liberties and national security. This ten-year debate is ongoing with key areas unresolved.

Legislative and Regulatory Measures

On Capitol Hill, Congress immediately reviewed and revised our national security policies, enacting the USA PATRIOT Act of 2001. This broad legislation included provisions that updated and modernized electronic surveillance laws; facilitated increased cooperation among federal, state and local law enforcement and intelligence agencies and, in some cases, granted more executive power to act on national security measures.

Meanwhile, President George W. Bush led an international military intervention in Afghanistan and acted on a range of apprehension and detention initiatives, redefining (and often narrowing) the rights of immigrants, foreign students, enemy combatants, and detainees. Moreover, Treasury Department officials devised a financial assault on terrorism through public designations of terrorists and terrorist supporters, the freezing of their accounts, and the application of economic sanctions.

While many were supportive of the government's legislative and regulatory measures, some were concerned that in the haste to make our nation more secure, basic civil and individual liberties were put in peril. The question of how best to balance civil liberties and national security was prominently borne out in a number of debates involving executive power in the past few years, including detention of prisoners at Guantanamo Bay, restricting material support for terrorists, and increased use of new surveillance warrants. This debate also played out in other contexts, from the creation of the Department of Homeland Security to the role of the Transportation Security Administration in protecting airports.

Detention of Prisoners at Guantanamo Bay

The Guantanamo Bay detention facility was established in 2002 by President Bush to hold detainees from the wars in Afghanistan and Iraq. Since its establishment, the policies of the United States concerning the facility have been scrutinized and challenged on numerous issues including: the unavailability of habeas relief for detainees, the inadequate access to effective counsel and inadequate Congressional oversight of tribunals. The Bush Administration argued that Guantanamo Bay could be considered outside U.S. legal jurisdiction and therefore the detainees were not entitled to the rights afforded prisoners in the United States, including habeas corpus. In addition, the Administration argued that the status of the detainees was such that the Geneva Conventions dis not apply. After a series of U.S. Supreme Court cases, culminating in the 2008 *Boumediene v. Bush*, the High Court reaffirmed the rights of detainees in American custody in Guantanamo Bay, Cuba, to challenge their indefinite detention. Notably, Guantanamo was just one entity in a new series of prisons, including a detention facility at Bagrahm Air Force in Afghanistan (which now holds more prisoners than at Guantanamo and which has been similarly criticized for detaining persons in violation of international law).

Significant debate has also focused on the executive branch's use of so-called "enhanced" interrogation techniques on prisoners, including waterboarding. One key debate focused on whether these techniques constituted torture.

In addition, these cases highlighted the real tension in determining the forum for prosecuting alleged enemy combatants and terror-related detainees arrested off of U.S. soil. While a suspect arrested in the United States is

67123.620

undoubtedly eligible for trial in a U.S. court, there is a very real debate over whether someone captured abroad by U.S. forces is entitled to be tried in the U.S. One solution, military tribunals and commissions, has been favored by both Presidents Bush and Obama. The key questions of this debate are whether detainees will get due process of law, how much due process is owed to such a detainee in the first place, what does international law require the U.S. to provide these so-called "enemy combatants" and whether and how U.S. courts will supervise, if at all, the administration of justice within this extra judicial system of trials and detention.

Providing Material Support for Terrorism

One of the government's most frequently used tools in the fight against terrorism is the provision of federal law that prohibits material support or resources to individuals or entities that facilitate, plan or engage in terrorism. For instance, in 2009, the Holy Land Foundation for Relief and Development, once considered the largest Muslim charity in the U.S., was shut down by the government for funding Hamas, which has been designated a terrorist group by the U.S. government. Some consider this provision crucial to combatting terrorism, arguing that even those that support a legitimate arm of an organization that promotes or engages in terrorism grants the organization legitimacy and frees up resources for the organization to engage in terrorist activities. Others have challenged the provision as being too vague and overbroad, and violating the free speech rights of Americans. In 2010, the U.S. Supreme Court (*Holder, et. al. v. Humanitarian Law Project, et. al,*) held that the provision was constitutional when the executive branch sought to limit technical training of a designated terrorist group.

The Use of Surveillance Warrants

A number of years after 9/11, it was revealed that the Bush Administration was engaging in warrantless wiretapping of U.S. citizens in their investigations of terrorist activity. Congress amended the Foreign Intelligence Surveillance Act to ease and expand the executive branch's use of electronic surveillance. While some thought this law was a needed change in order to combat terrorism in today's world of modern communication, others believed that the ease on warrant requirements, the leniency on recordkeeping and the immunity for telecommunications companies violate the individual liberties of Americans.

ADL's View of the Balancing of Individual Rights and National Security

In its dual role as an advocate of civil rights and liberties and an aggressive supporter of law enforcement's crucial role in protecting democracy and of the United States government's important efforts to fight domestic and international terrorism, ADL is uniquely qualified to analyze issues of national security and individual rights.

For decades, the League has been at the forefront of arguing for tougher anti-terrorism laws and monitoring the actions of extremist groups domestically and worldwide, including groups identified by the United States as foreign terrorist organizations. Such groups pose a threat to the very qualities that allow a diverse society to flourish as well as to the physical safety and security of Americans and others throughout the world. At the same time, ADL is an advocate of the First Amendment rights guaranteed under the United States Constitution.

ADL does not view balancing the two objectives of preserving civil liberties and securing national security as a zero sum game and has advocated for national policies that recognize the harsh reality of terrorism while maintaining key civil liberties protections, such as preserving the right to habeas corpus and ensuring that key provisions of the USA PATRIOT Act had expiration dates (sunset provisions) that would allow the debate over their propriety to continue anew. ADL supported enactment of the PATRIOT Act in October 2001 because we firmly believed that law enforcement and intelligence officials needed additional tools to identify, track, and prosecute terrorists and their supporters, and to prevent future attacks. From the outset, we stressed the importance of sunset provisions for certain parts of the act, and called for continuing robust Congressional oversight, accountability and transparency in implementing the powers granted under the Act, appropriate administrative reporting requirements and opportunities for meaningful judicial review of these provisions.

67123.621

Some of ADL's Key Actions

- Advocated for Congress to recalibrate the balance between security and individual rights following the rash of hate violence in the aftermath of the September 11 terrorist attacks.
- Supported passage of the USA PATRIOT Act – but called for key oversight and sunset provisions.
- Provided specialized training and expertise on extremism, hate groups, domestic and international terrorism, and civil liberties to high-level law enforcement personnel through ADL's Advanced Training School, and regional trainings, often with U.S. Attorneys.
- Conducted, in partnership with the United States Holocaust Memorial Museum (USHMM), Law Enforcement and Society (LEAS) training, which draws on the history of the Holocaust to provide law enforcement professionals with an increased understanding of their relationship to the people they serve and their role as protectors of the Constitution.
- Actively lobbied for strengthening America's anti-terror laws to enhance law enforcement's ability to prevent terrorism and meet a real and present threat.
- Addressed xenophobia and restrictive enforcement-only immigration initiatives. The League has strongly opposed proposals to direct local law enforcement officials to enforce federal immigration laws on the grounds that involvement of local authorities in these efforts would undermine public trust and obstruct effective community policing.
- Submitted amicus briefs arguing against indefinite detention at Guantanamo Bay, for full *habeas* rights of American citizens and for due process rights of enemy aliens detained in Iraq and Afghanistan. ADL believes that access to counsel and knowledge of the charges being brought against the accused are fundamental constitutional principles.
- Supported the ban on fundraising for designated foreign terrorist organizations, enacted as part of the Anti-Terrorism and Effect Death Penalty Act of 1996 (AEDPA), and has continued to file amicus briefs in successful litigation supporting the constitutionality of those aspects of the AEDPA.
- Submitted a friend-of-the-court brief to the U.S. Supreme Court in 2009 in a case entitled, *Holder, et. al. v. Humanitarian Law Project, et. al*, defending the constitutionality of material support for terrorism provisions of the Anti-Terrorism and Effective Death Penalty Act of 1996.
- Continued to raise awareness about the terrorist threat through ADL's Leon and Marilyn Klinghoffer Memorial Foundation and developed educational, political, and legal strategies to enhance the fight against terror worldwide with the support of the Foundation and ADL's William and Naomi Gorowitz Institute on Terrorism and Extremism.

The Anti-Defamation League, founded in 1913, is the world's leading organization fighting anti-Semitism through programs and services that counteract hatred, prejudice and bigotry.

67123.622

RIGHTS working group

STATEMENT OF

MARGARET HUANG, EXECUTIVE DIRECTOR
RIGHTS WORKING GROUP

HEARING ON TEN YEARS AFTER 9/11: ARE WE SAFER?

SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

TUESDAY, SEPTEMBER 13, 2011

Chairman Lieberman, Ranking Member Collins, and members of the Committee: I am honored to submit this testimony for the record on behalf of Rights Working Group regarding today's hearing on "Ten Years After 9/11: Are We Safer?" Formed in the aftermath of September 11th, Rights Working Group (RWG) is a national coalition of over 300 organizations from across the country representing civil liberties, national security, immigrant rights and human rights advocates. RWG seeks to restore civil liberties and human rights protections that have eroded since 9/11, ensuring that the rights of all people in the U.S. are respected regardless of citizenship or immigration status, race, national origin, religion or ethnicity. Currently, RWG leads the Racial Profiling: Face the Truth Campaign which seeks to win reforms to end various forms of racial and religious profiling. RWG is particularly concerned about national security policies which encourage discriminatory law enforcement practices such as racial profiling and violate the civil and human rights of persons living in the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00997 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.623

RIGHTS working group

September 11th, 2011 was a profoundly tragic day in history that irrevocably altered our nation. Almost 3,000 lives were lost in New York, Washington DC and Pennsylvania. First responders working in the toxic air surrounding the wreckage of the World Trade Center fell ill and some died as a result of their illness. The families and loved ones left behind still feel that loss today.

As the country reflects on this day we should also reflect on national-security policies enacted after 9/11 and consider another significant loss—the loss of civil liberties and human rights protections for many communities in the U.S. Many post 9/11 national security policies created a perception of tough government responses that ensured security for those living in the United States. Instead, many of these policies made us *less* safe: they have distracted law enforcement and intelligence resources away from targeted, behavior-based investigation and they have stripped people of their constitutional and human rights.

National Security Measures and Racial Profiling

After Japan's bombing of Pearl Harbor, more than 120,000 Americans of Japanese descent were rounded up and sent off to internment camps. This detention, done in the absence of individualized suspicion and without due process, is one of the most shameful examples of racial profiling in recent U.S. history. Rather than saying "never again", after 9/11, the U.S. government reenacted suspicion-less targeting of individuals—this time of those who were of Arab, Middle Eastern, Muslim and South Asian and citizens of Arab, Middle Eastern, Muslim and South Asian descent. Racial profiling expanded dramatically under a number of new or revised government policies and programs. Members of Arab, Middle Eastern, Muslim and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00998 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.624

South Asian communities were increasingly and disproportionately placed under surveillance, stopped, searched, interrogated, detained and labeled "terrorism suspects." The government also began aggressively using civil immigration laws, criminal laws and criminal procedure in a sweeping and discriminatory manner to target members of these communities—as well as of members of Latino communities in the name of border and homeland security.

Racial Profiling at Border Stops and Searches

In the years that have followed Sept. 11, 2001 Arabs, Middle Easterners, Muslims and South Asians and citizens of Arab, Middle Eastern, Muslim and South Asian descent continue to be singled out for intrusive questioning, invasive searches and lengthy detentions without reasonable suspicion of criminal activity. Customs and Border Protection (CBP) agents question individuals about their faith, associations and political opinions. Travelers' personal documents, books, laptop computers, cell phones and other electronic devices have been seized and, some believe, copied by CBP agents.[1] This unjust treatment is due partly to a general CBP guidance released in 2008 that allows officers to "review and analyze information transported by any individual attempting to enter, reenter, depart, pass through, or reside in the United States" without individualized suspicion.[2]

[1] Asian Law Caucus & Stanford Law School Immigrants' Rights Clinic. "Returning Home: How U.S. Government Practices Undermine Civil Rights at Our Nation's Doorstep", 2009, *available at* <http://www.asianlawcaucus.org/wp-content/ uploads/2009/04/Returning%20Home.pdf>. See also: Muslim Advocates."Unreasonable Intrusions: Investigating the Politics, Faith & Finances of Americans Returning Home", 2009, *available at* <http://www.muslimadvocates.org/documents/Unreasonable_Intrusions_2009.pdf>

[2] United States Custom and Border Protection, Department of Homeland Security, "Policy Regarding Border Search of Information," July 16, 2008, <http://www.customs.gov/linkhandler/cgov/travel/admissibility/search_authority.ctt/search_authority.pdf>.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 00999 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.625

RIGHTS working group

Racial Profiling at Airports

The Transportation Security Administration (TSA) has faced ongoing allegations of discriminatory enforcement since its inception. Members of the Arab, Middle Eastern, Muslim and South Asian community and citizens of Arab, Middle Eastern, Muslim and South Asian descent report being "randomly selected" for secondary screenings almost every time they go to the airport. These searches are more than mere inconveniences. Some individuals are delayed for their flights—missing vacations or professional conferences— while others are subjected to invasive and humiliating searches, sometimes in full view of the public and struggle against the stigma of being unjustly labeled a terrorist suspect.

In August 2007, TSA released new guidelines to serve as standard operating procedures for airport security screening. People with Sikh turbans and Muslim head coverings were singled out for screening with higher scrutiny, despite a lack of evidence that these religious head coverings were being employed to hide dangerous items. Widespread profiling of Sikhs occurred as a result, and the Sikh Coalition, an advocacy group, found that nearly all turban-wearing Sikh men were subjected to additional screening.[3] In late 2007, a set of options for screening Sikhs that allows, for example, greater privacy, was negotiated by the TSA and Sikh organizations in coordination with the release of TSA's October 2007 "bulky clothing" policy.[4] But in practice, this new policy under which "passengers could be subjected to additional screening to further evaluate any item that could hide explosives or their components"[5] has unfortunately resulted in

[3] The Sikh Coalition. "The TSA Report Card: A Quarterly Review of Security Screenings of Sikh Travelers in U.S. Airports", Aug. 2009.
[4] The Sikh Coalition "TSA Develops New Procedure for Screening Turbans at U.S. Airports", Oct 17, 2007, <http://www.sikhcoalition.org/advisories/TSADevelopsNewProcedure.htm>.
[5] Transportation & Security Administration. TSA's Head-to-Toe Screening Policies, Oct 15, 2007, <http://www.tsa.gov/press/happenings/sop_facts.shtm>

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01000 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.626

the continued targeting of this community as well as others, such as Muslim women who wear *hijab*, a religious head covering traditionally worn by Muslim women, or other head coverings.

This practice of over-searching, although perhaps appearing to increase security, does not achieve that objective. As Sheldon Jacobson, a University of Illinois computer science professor with expertise in aviation security has said, "Ironically, more screening can result in less security when it directs attention and resources to the 60 to 70 percent of people who are not a security threat. That, in turn, diverts attention and resources away from the people who are a legitimate threat.... By lavishing billions of dollars on screening the wrong passengers, we're not spending those dollars on the right passengers. Since it takes only one successful act of terrorism for the system to fail, we cannot afford to allocate our finite amounts of time, money and technology in the service of a failed strategy."[6] Instead of helping effectively target legitimate security threats, over-screening—particularly based on race, ethnicity, religion and national origin—has the opposite effect.

NSEERS and Operation Frontline

Another government initiative adopted after September 11, 2001 was the National Security Entry-Exit Registration System (NSEERS) which employed immigration law as a counter-terrorism tool. This program required nonimmigrant males aged 16 to 45 from 25 countries to register for fingerprinting, photographs, and lengthy interrogations. All but one of the countries were predominantly Muslim; the anomaly was North Korea. More than 80,000 men underwent registration and thousands were subjected to lengthy interrogations and detention. Many individuals were deported through secret proceedings that took place without due process of law.

[6] Sheldon Jacobson, interviewed by Phil Ciciora. News Bureau, Jan. 7, 2010, .<http://illinois.edu/lb/article/72/33799>.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01001 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.627

However, not one single terrorism conviction resulted from this program. An investigation by the National Commission on Terrorist Attacks upon the United States determined that programs like NSEERS did not demonstrate clear counter-terrorism benefits.[7] They instead instilled fear in families and communities, creating a distrust of law enforcement and the government, and isolating Arab, Muslim, Middle Eastern and South Asian communities.

Additional government programs such as "Operation Frontline," initiated just prior to the 2004 election cycle and designed to "detect, deter and disrupt terrorist operations," utilized the NSEERS database to identify targets.[8] Data from DHS revealed that 79 percent of individuals investigated were from Muslim majority countries.[9] The timing of this program further fueled community distrust in government and had a chilling effect on voters of Arab, Middle Eastern, Muslim and South Asian descent.

In April of this year, the Department of Homeland Security announced that citizens of countries subject to NSEERS would no longer be required to register. However, the NSEERS infrastructure remains intact. This policy shift does not address the many individuals who are currently facing removal or a denial of immigration benefits. RWG urges the Committee to work with the Administration to ensure that favorable discretion is exercised toward individuals facing immigration consequences because of an NSEERS-related issue. Furthermore, the Committee should urge the Administration to terminate this failed and discriminatory program in its entirety.

---

[7] Thomas R. Eldridge et al. '9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks upon the United States", 2004.
[8] American–Arab Anti-Discrimination Committee and Yale Law School. "ICE Targets Immigrants from Muslim Majority Countries Prior to 2004 Presidential Election", October 20, 2008.
[9] Eric Lichtblau, "Inquiry Targeted 2,000 Foreign Muslims in 2004", *N.Y. Times*, Oct. 30, 2008, at A17, available at http://www.nytimes.com/2008/10/31/us/31inquire.html.

287(g) and Secure Communities

Latino communities have also been ensnared by programs described as national-security or border security efforts such as the 287(g) and Secure Communities programs. The 287(g) program allows Immigration and Customs Enforcement (ICE) to deputize state and local law enforcement agents to enforce civil immigration laws. Research by independent sources indicates that 287(g) programs lead to racial profiling and that DHS is unable to provide oversight and guidance to local officers deputized under this program.[10] A DHS Office of Inspector General report described the misguided actions of one 287(g) officer: "an ICE supervisor described a situation in which a state highway patrol officer transported an accident victim to a participating county jail to determine the victim's immigration status. The ICE supervisor explained that the accident victim was not brought to the jail to be charged with an offense, but to have a 287(g) officer determine the victim's deportability. The victim was detained until a 287(g) officer could respond."[11]

The overwhelming evidence supports the immediate termination of the 287(g) program and the granting of redress to victims of racial profiling and others civil rights and civil liberties violations.

The Secure Communities program requires fingerprints that state or local law enforcement send to the FBI to be checked against DHS civil immigration databases to determine whether a person can be deported. Secure Communities creates an incentive for state and local law enforcement agents to arrest people for pre-textual reasons so that their immigration status can be checked

[10] *See* Mai Thi Nguyen and Hannah Gill, "The 287(g) Program: The Costs and Consequences of Local Immigration Enforcement in North Carolina Communities," The University of North Carolina at Chapel Hill, Feb. 2010 *available at* http://isa.unc.edu/migration/287g_report_final.pdf. *See also* Migration Policy Institute "Delegation and Divergence: A Study of 287(g) State and Local Immigration Enforcement," Jan. 2011 *available at* http://www.migrationpolicy.org/pubs/287g-divergence.pdf.
[11] DHS OIG Report at 32.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01003 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.629

during the booking process. DHS has stated that Secure Communities is funded to identify and remove criminal aliens, "the worst of the worst." However, ICE's own data demonstrates that 29% of individuals removed through the Secure Communities Initiative had no criminal record and that another 31% of individuals removed had a conviction for only the lowest level offenses.[12] In fact, only 26% of individuals removed had been convicted of Level 1 crimes.[13] This data reveals a complete divergence from the program's stated purpose and its outcomes.

Recently, through FOIA litigation, evidence has come to light demonstrating that DHS may have acted improperly in presenting the Secure Communities program to local communities, Congress, and the public.[14] DHS misrepresentation surrounding the ability of jurisdictions to effectively opt-out of the program has resulted in an ongoing audit of Secure Communities by the DHS Office of the Inspector General as well as a review by the GAO. [15] The rapid expansion of the program should be stopped unless and until proper and effective civil rights and civil liberties safeguards are established.

Fusion Centers and Suspicious Activity Reporting

Fusion centers—a key component of the DHS and DOJ's border and homeland security efforts—and the reliance on Suspicious Activity Reports are also of great concern. Fusion centers are local, state, and federal information gathering centers that evaluate, analyze and distribute

[12] Secure Communities Monthly Statistics through February 28, 2011 at p. 2 *available at* http://www.ice.gov/doclib/foia/sc-stats/nationwide_interoperability_stats-fy2011-feb28.pdf

[13] *Id.*

[14] "Congresswoman calls for investigation of enforcement program that screens for illegal immigrants in jails," *LA Times*, Apr. 22, 2011 *available at http://latimesblogs.latimes.com/lanow/2011/04/congresswoman-calls-for-investigation-of-enforcement-program-that-screens-for-illegal-immigrants-in-.html.*

[15] *See* Letter from Ranking Member of Subcommittee on Immigration Policy and Enforcement to DHS Office of the Inspector General and ICE Office of Professional Responsibility, dated Apr. 28, 2011 *available at* http://www.docstoc.com/docs/78191508/Lofgren-letter-to-DHS-IG. *See also* —Sen. Menendez in Support of Rep. Lofgren's Call for an Investigation into DHS's Implementation of Secure Communities Program,I Apr 28, 2011 *available at* http://menendez.senate.gov/newsroom/press/release/?id=7948683e-ad67-4141-9d4b-e0fa98af4456.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01004 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.630

individuals' personal information. There are currently (as of August 2011) at least 72 fusion centers around the country.[16] Fusion centers partner with nontraditional data collectors, such as public safety entities and private sector organizations which possess information such as financial holdings, litigation history, employment references, and suspicious activity reports. Fusion center personnel can request or require local law enforcement to collect and report information on individuals based on racial and other identity-based profiling. Meanwhile, Suspicious Activity Reports (SARs) which encourage policing by private citizens have been promoted through efforts such as the DHS' "See Something, Say Something" campaign. An extraordinary number of collected SARs were based on race, ethnicity, national origin, or religious affiliation—or failed to demonstrate that there was a reasonable connection between the behavior and a criminal activity. In other words, these SARs yielded information that law enforcement is not supposed to record or use—but it was collected and stored anyway. To put the scope of the problem in perspective, a 2010 DOJ evaluation found that the two local programs highlighted in the review–Florida and Virginia – failed to meet information collection standards 98% (Virginia) or 99.8% (Florida) of the time.[17]

Much of this unlawful racial profiling of ethnic communities—through the reliance on CBP and TSA screenings, local law enforcement involved in federal immigration law, suspicious activity reports, fusion centers at the border and the interior of the United States and special registration

[16] National Network of State and Major Urban Area Fusion Centers, available at http://www.ise.gov/national-network-state-and-major-urban-area-fusion-centers.

[17] Bureau of Justice Assistance, *Final Report: Information Sharing Environment Suspicious Activity Reporting Evaluation*, 32 (2010), http://nsi.ncirc.gov/documents/NSI_EE.pdf.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01005 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.631

programs— has resulted in a heightened fear of law enforcement in immigrant communities and communities of color in the US.

As a result, community groups have reported that members of targeted ethnic communities became so afraid of having any contact with officials after post-9/11 "national security" or "counter-terrorism" policies were introduced that they did not report emergency situations, such as domestic violence and other crimes—and, in some cases, did not seek medical treatment.[18] A 2006 study commissioned by the DOJ established that Arab Americans were significantly fearful and suspicious of federal law enforcement due to government policies. It also determined that both community members and law enforcement officers defined diminished trust as the most important barrier to cooperation.[19] Similar effects are also found in Latino communities where local law enforcement are implicated in federal immigration enforcement efforts— community members are terrified of coming forward as witnesses or victims of crimes when they fear immigration consequences for themselves or their family members.

Conclusion

At a time when Americans have felt most vulnerable, these "national security" efforts created an illusion of safety, but actually have the opposite effect. Counter-terrorism strategies that target people because of their race, ethnicity, religion or national origin have failed. Racial profiling in the name of national security diverts precious law enforcement resources away from smart, targeted investigations and toward dragnet techniques that strip many people of their constitutional and human rights. Former Homeland Security Secretary Michael Chertoff

[18] Immigration Policy Center "Targets of Suspicion: The Impact of Post-9/11 Policies on Muslims, Arabs and South Asians in the United States", 2004, <http://ispu.org/reports/articledetailpb-63.html>
[19] Vera Institute of Justice. "Law Enforcement and Arab-American Community Relations after September 11, 2001: Engagement in a Time of Uncertainty", pp. 13, 21, 2006, <http://www.vera.org/download?file=147/Arab%2BAmerican%2Bcommunity%2Brelations.pdf>

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01006 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.632

highlighted the ineffectiveness of profiling based on national origin in the days after the 2009 Christmas Day bomb attempt. He said: "Well, the problem is that the profile many people think they have of what a terrorist is doesn't fit the reality. Actually, this individual probably does not fit the profile that most people assume is the terrorist who comes from either South Asia or an Arab country. Richard Reid didn't fit that profile. Some of the bombers or would be bombers in the plots that were foiled in Great Britain don't fit the profile. And in fact, one of the things the enemy does it to deliberately recruit people who are Western in background or in appearance, so that they can slip by people who might be stereotyping. So, I think the danger is, we get lulled into a false sense of security, if we profile based on appearance. What I do think is important is to look at behavior. And that's something that we are doing and should continue to do more of."[20]

Ten years later after 9/11, the Rights Working Group coalition sees the anniversary of these events as a chance for the U.S. to pause and remember—to reflect on the losses since September 11th and to reclaim those rights lost in the aftermath of the attacks. The U.S. government should emphasize the values that reflect the best intentions of this country's history—democratic governance, embracing diversity and equal justice under the law. While grieving the losses felt by so many after the tragic deaths of September 11th, let the anniversary serve as a call to action to reaffirm and restore the fundamental commitment that the human rights and civil liberties of all people must be upheld.

[20] Campbell Brown "Investigating the Christmas Day Terror Attack: Obama Administration Downplaying War on Terror?", CNN, Dec. 30, 2009, <http://transcripts.cnn.com/TRANSCRIPTS/0912/30/ec.01.html>.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01007 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.633

RIGHTS working group

The government should never use a tragedy as an excuse to sacrifice civil and human rights. The United States should continue to aspire to fulfill its mission of providing liberty and justice for all. Freedom and Security can co-exist in the United States and the next 10 years should be about restoring constitutional and human rights. To this end, Rights Working Group recommends:

- Congress should introduce and pass the "End Racial Profiling Act" instating a federal ban on profiling based on race, religion, ethnicity and national origin at the federal, state and local levels.

- Congress should urge DHS to fully repeal all NSEERS-related regulations and ensure that favorable discretion is exercised toward individuals facing immigration consequences because of an NSEERS-related issue. The Committee should urge DHS to purge all information gathered through this discriminatory program.

- The Committee should investigate the devolution of immigration authority to state and local law enforcement through programs like 287(g) and Secure Communities and call for the federal government to reassert full responsibility for enforcing immigration law and creating immigration policy.

- The Committee should ensure that DHS immigration enforcement policies comply with civil and human rights laws and urge DHS to create effective safeguards to prevent racial profiling and other rights violations. The Committee should ensure that these standards apply to all components of DHS, including CBP and TSA.

- The Committee should ensure that DHS border programs and policies do not promote racial profiling or other civil rights violations.

- Committee members should urge the Department of Justice to revise its 2003 racial profiling guidance to eliminate the loophole that allows racial and religious profiling in

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01008 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.634

the name of national security and speak out against policies that target Muslim communities.

Thank you again for this opportunity to express the views of the Rights Working Group coalition. We welcome the opportunity for further dialogue and discussion about these important issues.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01009 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.635

Senator Jay Rockefeller IV
Statement for the Record
"Ten Years After 9/11: Are We Safer?"
Hearing of the Senate Committee on Homeland Security and Governmental Affairs
September 13, 2011

I am sorry I am unable to join you for this hearing at the Homeland Security and Governmental Affairs Committee. But I want to thank the distinguished Chairman, Senator Lieberman, and Ranking Member, Senator Collins, for holding this hearing on such an important topic—at such an important time. Let me also thank the stellar panel of public servants—Secretary of the Department of Homeland Security, Janet A. Napolitano; Director of the Federal Bureau of Investigation, Robert S. Mueller III; and Director of the National Counterterrorism Center, Matthew G. Olsen. I am grateful for their service and the work they do to protect us from harm and preserve our freedom.

This weekend our nation marked the tenth anniversary of 9/11. Today, this Committee asks if ten years hence we are as a people and a country safer.

In many ways, I believe we are more secure. There may be no clearer evidence than the absence of a major attack on our soil during the last decade. Abroad, we have disrupted the terror network led by Osama bin Laden.

But in others, I fear, we have fallen short. As the 9/11 Commission Report noted, the inability of our first responders to communicate was a critical failure on that fateful day. There is no doubt it contributed to the tragedy and loss of life.

Ten years later, as we honor the tremendous bravery of our public safety officials, it is long past due to provide them with the communications tools they need to do their jobs. Every day they are on the front lines. They protect our neighborhoods and communities. They respond fearlessly when the unthinkable occurs. But too often they lack the interoperable networks that are essential to providing an effective response in emergencies. They lack the ability to communicate with one another, with other agencies, and across city and state lines. This hampers our ability to respond to a crisis. Whether that crisis is a terrorist attack or natural disaster, it puts lives in unnecessary danger.

It is not too late to do something about it. With my colleague on the Senate Committee on Commerce, Science, and Transportation, Ranking

67123.636

Member Kay Bailey Hutchison, I have been working to pass S. 911, the Public Safety Spectrum and Wireless Innovation Act. This bipartisan legislation would implement a nationwide, interoperable wireless broadband communications network for our first responders.

This bill would do two key things.

First, it would set aside 10 megahertz of 700 MHz spectrum known as the D-block for public safety officials. This will facilitate communications for our first responders across the country—no matter who they are, or where they are asked to serve, on the same swath of airwaves.

Second, it would give the Federal Communications Commission the authority to hold incentive auctions based on the voluntary return of spectrum. These auctions, in turn, will provide funding to support the construction and maintenance of a public safety network using 700 MHz spectrum. It also will free up additional spectrum for innovative commercial uses. In an industry that has created 420,000 new jobs over the past decade, this bill is crucial to that continued growth.

In short, this bill marries much needed resources for first responders with smart commercial spectrum policy. It can help keep us safe in a world where the threats to our security are too numerous to count. It can help grow our wireless economy, too. And to those who say we cannot afford to do this now, I say we cannot afford not to. Because this effort is about saving lives. But if this reason is not compelling enough, it is important to know this: this legislation pays for itself. According to the nonpartisan Congressional Budget Office, incentive auctions will bring in revenue well above what funding public safety requires, leaving billions over for deficit reduction.

So as we come together as a nation to remember and honor the lives lost ten years ago, and as this Committee comes together to ask about our safety in the days ahead, I want to urge my colleagues to support the Public Safety Spectrum and Wireless Innovation Act.

Finally, I want to note that I am grateful for the interest that Senator Lieberman and Senator McCain have shown in this issue, with their legislation involving first responders and spectrum. I look forward to continuing to working with them—and provide our brave public safety officials with the communications they deserve and the resources they need to help keep us safe.

67123.637

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Joseph I. Lieberman

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

Question#:	1
Topic:	information
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: How would you assess the effectiveness of efforts by DHS and FBI to disseminate threat information to state, local, tribal and private sector entities with respect to the threat stream tied to the tenth anniversary of 9/11? What "lessons learned" do you have from this process with respect to dissemination of terrorism threat information in the future? (Note: Question also submitted to Director Mueller; may provide joint DHS-FBI answer if appropriate).

Response: Coordination between the FBI and DHS has improved significantly under this Administration. DHS and the FBI have partnered on product development and dissemination, outreach to State and Locals, and other information sharing efforts. These included:

- Development of several dual sealed bulletins;
- Several FBI/DHS-led SVTCs held for Field Offices, State and Major Urban Area Fusion Center Directors, Major Cities Chiefs and Homeland Security Advisors;
- Several Incident Community Coordination Team (ICCT) calls with communities in NY and DC;
- Multiple Briefings for State and Local law enforcement, and private sector partners; and
- Joint education materials for the public on the "If You See Something, Say Something ™" public awareness campaign.

DHS and the FBI executed a joint intelligence dissemination campaign to notify State, local, tribal, territorial and private sector entities of the 9/11 anniversary threat information. In the days leading up to the 9/11 anniversary, DHS and the FBI produced several Joint Intelligence Bulletins (JIBs) to ensure that law enforcement and civil authorities deployed appropriate resources to address any potential threat, before any specific threat reporting was available. Subsequently, specific threat information was received, and State, local, tribal, and territorial stakeholders were briefed on the threat stream through a series of conference calls, meetings, and dissemination of tear line

67123.638

Question#:	1
Topic:	information
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

intelligence products. The DHS Office for Civil Rights and Civil Liberties (CRCL) also convened the ICCT security and threat assessment conference calls for community organizations and coalition groups to allay concerns that their constituencies would be disparately impacted by activities leading up to the 10th anniversary of 9/11.

As more details became available, DHS and the FBI released a series of JIBs to its State, local, tribal, territorial, and private sector partners outlining the nature of the threat and recommending counter-measures. Briefings to State and Major Urban Area Fusion Centers Directors, Homeland Security Advisors, Major Cities Chiefs, State and local law enforcement, and private sector partners involved use of the information contained in the JIBs. Within the Fusion Center environment, deployed DHS Intelligence Officers coordinated actions with JTTF representatives and FBI Headquarters to ensure that DHS stakeholders received updated intelligence throughout the time of the threat. DHS and the FBI followed up a week later with an "enduring threat" JIB to remind law enforcement to remain vigilant after the 9/11 anniversary.

Preparation for the 10th anniversary of September 11th was an exercise in applying the lessons learned about information sharing since 9/11. As a result of those lessons learned, DHS and the FBI have worked to build more robust information sharing mechanisms, and to create a more vigorous communication structure that allows for more effective dissemination of threat information to State, local, tribal, territorial, and private sector partners. DHS will continue to develop a close working relationship with the FBI to help ensure that DHS partner agencies receive a clear, consistent, and accurate assessment of all threats to the Homeland.

67123.639

Question#:	2
Topic:	fusion centers
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Secretary Napolitano, in your testimony you emphasize the importance of state and local fusion centers as part of our national efforts to prevent and disrupt homegrown terrorism. These fusion centers are still a work in progress and their capabilities are uneven, but my view is that they've taken important steps toward maturity under your leadership. As you're well aware, there were significant cuts to funding for homeland security grants in the FY 2011 budget for DHS, and further cuts are being contemplated by the appropriators for FY 2012. These grant programs are the primary source of federal funding for fusion centers, so there is a real risk that we could see many of them would halt or reverse the progress they have made as the result of grant cuts.

What will be the impact of homeland security grant cuts to the national network of fusion centers? What is the Department doing to address these concerns and mitigate this impact?

Response: Over the past three years, we have made tremendous progress in building a grassroots analytic capability through the National Network of Fusion Centers that not only directly impacts State and Local efforts to prevent crime but also supports our national capability to protect the Homeland from potential attacks.

While significant reductions in grant funding in both FY 2011 and FY 2012 will certainly have impact on the level of direct financial support DHS can provide to state and local partners, DHS recognizes the importance of fusion centers in our antiterrorism efforts and will continue to prioritize grant funding to support fusion center development and activities through both State Homeland Security Grants and UASI Grants.

In FY2011, the Maturation and Sustainment of the National Network of Fusion Centers was identified as one of the overarching grant priorities. DHS required that those States and urban areas with recognized fusion centers must include at least one investment justification (IJ) that addresses funding support for the fusion center. This represents the first time that an IJ has been required for a specific priority mission activity. The IJ must also be tied to mitigating capability gaps in a fusion center's operation, as identified in the Baseline Capabilities Assessment (BCA). Additionally, grantees are now required to submit the results of the BCA with their grant applications to ensure that requested funds are adequately tied to identified capability gaps.

Going forward, DHS is committed to ensuring that fusion centers remain a priority; that grant requests are tied to capability gaps; and, that other DHS grant programs provide flexibility to support the all-hazard missions of fusion centers. DHS will also continue to work with its Federal partners, including DOJ's Bureau of Justice Assistance, DOJ's Office of Community Oriented Policing Services, and the Centers for Disease Control and Prevention to continue to build on the successes of FY 2011, and to strengthen their respective grant programs in support of fusion center activities.

67123.640

Question#:	3
Topic:	CVE
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Many of the Department's agencies should play an important role in countering violent Islamist extremism. For example, DHS' Civil Rights and Civil Liberties Office conveys roundtables with Muslim Americans, US Citizenship and Immigration Services is sometimes the first real interaction with the government that new citizens have, and the DHS Office of Intelligence and Analysis is tasked with getting state and locals the right information on the nature of the threat, which should clearly different between violent Islamist extremism and Islam.

Who is the lead at DHS for preventing violent Islamist extremism?

Response: To coordinate the Department's CVE efforts, regardless of ideology, the Secretary for Homeland Security established the DHS Countering Violent Extremism Working Group (CVEWG) to better coordinate the Department's operational and programmatic efforts to prevent and protect against foreign and homegrown terrorist attacks. The Working Group is comprised of leadership representation from all of the Department's operational components and offices that have equities in CVE. John Cohen, Senior Advisor to the Secretary Chairs the CVEWG and is responsible for leading CVE efforts across the Department.

Question: Please define the mission and purpose of DHS' CVE program.

Response: In August 2011, President Obama released the *National Strategy on Empowering Local Partners to Prevent Violent Extremism ("the Strategy")*, which is a whole of government approach to address CVE. Following this, in December 2011, the Administration released the *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States (SIP),* detailing how the Administration would implement the *Strategy.* The SIP identified DHS as the lead or partner agency for a majority of the government's planned CVE activities.

The DHS approach to CVE emphasizes the strength of local communities, beginning with the premise that well-informed and well-equipped families, communities, and local institutions represent the best defense against terrorist ideologies. DHS works with its Federal, State, Local, Tribal, and Private Sector partners to prevent violence that is inspired by individuals or groups with extremist ideologies, irrespective of whether these individuals come to this country from abroad or if they come from the U.S. The Department's priority as it relates to CVE is to address violent extremism that is linked to al-Qa'ida and its affiliates and/or inspired by al-Qa'ida's ideology. While addressing

67123.641

Question#:	3
Topic:	CVE
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

violent extremist activity inspired by the al-Qa'ida philosophy is the Department's top priory the Department's approach to CVE is adaptable to all ideologically motivated violence. DHS works with a broad range of partners to gain a better understanding of the behaviors, tactics, and other indicators that could point to potential terrorist activity within the United States. DHS also works with these partners on best ways to mitigate or prevent terrorist activity.

The Department's CVE efforts are three-fold:

1) Support and coordinate efforts to better understand the phenomenon of violent extremism, including assessing the threat it poses to the Nation as a whole and within specific communities;

2) Bolster efforts to catalyze and support non-governmental, community-based programs and strengthen relationships with communities that may be targeted for recruitment by violent extremists; and

3) Disrupt and deter recruitment or individual mobilization through support for local law enforcement programs, including information-driven, community-oriented policing efforts that have been proven effective in preventing violent crime for decades.

Question: Please provide any metrics the Department uses to assess the effectiveness of CVE programs, including any written documentation.

Response: The metrics we currently apply focus largely on assessing how effectively the Department is developing and delivering a range of CVE-related programs. These include keeping track of the number of engagement efforts, trainings, information and research product delivered; and the scope of information sharing.

Question: What is the budget for CVE programs? Please provide a breakdown by each office and program.

Response: The Department is integrating its approach to CVE into the day to day activities of its operational Components. In some cases, specific CVE efforts are closely aligned from a budgetary perspective. In other cases, activities supportive of efforts to address violent extremism are integrated into in the core operational budgets. The Department's CVE efforts do not have a specific budget line item, and offices do not have specific funding streams solely used for CVE. However, there are programs that leverage the existing capabilities of the Department to accomplish its CVE goals.

67123.642

Question#:	3
Topic:	CVE
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Please list all programs and offices that perform CVE functions and their individual missions and functions as it relates to CVE.

Response: DHS is integrating CVE into all relevant offices, and raising broader awareness of the issue across the Department. By doing so, DHS leverages its existing programs, resources, and relationships for direct and indirect CVE purposes.

Question: How many personnel are assigned full time to CVE efforts? How many part-time?

Response: As previously stated, the Department is in the process of integrating CVE into all relevant offices. For example, the Department's Office for Civil Rights and Civil Liberties (CRCL) is a major engagement arm of DHS. While CRCL offers training to law enforcement on cultural awareness and how to better engage with communities, it also focuses on broader engagement with diverse communities and grievance issues. CRCL's mission and programs do not solely focus on CVE; however, it leverages its existing capabilities to address direct and indirect CVE issues. In regards to staff, the internal DHS Countering Violent Extremism Working Group (CVEWG) is the body that coordinates all CVE effort and advises how to best leverage the Department's capabilities. It has participants from all of the DHS components. The working group also illustrates that every component and office within the Department of Homeland Security has a role in countering violent extremism. The Secretary has continued to stress the critical role the Department plays in this arena and she has placed a high priority on those efforts.

Question: Do you agree that countering violent Islamist ideology presents a different and specific challenge than "violent extremism" as a whole, and that the Department should tailor its programs to address that preeminent threat?

Response: The Department's priority as it relates to CVE is to address violent extremism that is linked to al-Qa'ida and its affiliates and/or inspired by al-Qa'ida's ideology. The Department's approach to countering violent extremism (CVE) is applicable to all ideologically motivated violence in that it focuses on empowering local communities and informing state, local, tribal and territorial law enforcement officials with the resources, training and information needed to detect and prevent violent attacks by those inspired by extremist ideological beliefs.

67123.643

Question#:	4
Topic:	NPPD
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Committee was briefed in early June on plans for the reorganization of the National Protection and Programs Directorate. Since then, the Committee has received little information about the nature of those plans and the steps taken to implement the proposed reorganization. What are the current plans to reorganize NPPD and when will those plans be implemented? Additionally, will those plans require congressional action and will they be consistent with relevant provisions contained in the Department of Homeland Security Authorization Act of 2011, recently approved by this Committee?

Response: The National Protection and Program Directorate's (NPPD) growing operational and mission support responsibilities have changed the nature of what was once a 400-person Department of Homeland Security (DHS) Headquarters element. Today, through continual growth and the addition of the Federal Protective Service, NPPD has more than 2,600 Federal employees and a contract workforce of nearly 15,000. It has a national footprint, with offices in 236 cities and a field workforce of more than 1,700 employees responsible for assessing the security and resiliency of Federal, chemical, and other private sector facilities; providing law enforcement and security services to over 9,000 Federal facilities; and working to protect the Nation's infrastructure, both critical physical and cyber.

NPPD's organizational planning efforts are focusing on changes that would more closely align cybersecurity and physical infrastructure protection and resilience efforts. The goal is to achieve synergies and efficiencies by clarifying roles and responsibilities and a more integrated approach to the execution of both operational and business support functions. NPPD plans to optimize current resources by:

- Integrating and aligning NPPD's work in key areas (private sector interactions, risk assessments, and regulatory matters) in an all-hazards approach and renewing our focus on driving the outcomes of increased security and resiliency for infrastructure. This will result in a more streamlined and nimble organization that is more capable of responding to physical and cyber threats.
- Establishing a focused and integrated analysis and risk management capability that will drive NPPD programs across its mission space and provide more value to the Federal, state, local, and private sectors.
- Aligning and aggregating resources and people across business and mission support functions.

67123.644

Question#:	4
Topic:	NPPD
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

NPPD continues to plan the transition and recognizes the importance of Congressional engagement in the process. NPPD's transition efforts are focused around two main objectives. The first objective is to realign NPPD mission functions to become a more risk-driven, knowledge-focused organization to better accomplish our mission. The second is to align and aggregate NPPD business and mission support functions to better support and meet our operational mission requirements. In order to determine how best to accomplish these objectives, NPPD has taken the following steps:

- During the summer of 2011, NPPD established a Transition Management team to oversee transition plans and ensure the necessary resources and skills are available to support the transition effort. The team is headed by two full-time executives with experience in change management, personnel, and program management.
- The transition team is augmented by operational, business, and mission experts who lead working groups in the areas of stakeholder engagement, analytics, and institutional capacity to help drive functional alignment and business support integration.
- To ensure that all NPPD subcomponents have insight and involvement into areas that will affect them, an NPPD Deputy Directors Board was established to promote cross-component involvement and to provide input, feedback, and recommendations to senior leadership on topics that impact NPPD across internal functional areas. The Board is currently working through organizational structures and mission alignment recommendations developed by the working groups for the transition.

Senior NPPD leadership will be briefed on recommendations presented by the working groups, which will then be presented to the Department's leadership for approval. The Department looks forward to working with the Committee to ensure that provisions of all appropriate DHS Authorization Acts are consistent with our planning efforts. We will continue to keep Congress informed on these efforts.

67123.645

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Daniel K. Akaka

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

Question#:	5
Topic:	structure
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: Section 213 of S. 1546, the Department of Homeland Security Authorization Act of 2011, would require the Secretary of the Department of Homeland Security to designate an official of the Department to coordinate efforts to counter violent extremism in the United States, including the ideology that gives rise to Islamist terrorism as identified in the 9/11 Commission Report.

Please explain the Department's current structure for coordinating efforts to counter violent extremism in the United States, including whether Section 213 would enhance the Department's efforts or whether the Department already has the appropriate structure in place.

Given that Section 213 would statutorily mandate that the Department focus its powers on the particular ideology that gives rise to "Islamist" terrorism, what affect, if any, would this Section have on the Administration's efforts to build trust and a cooperative relationship within the Muslim community?

How would Section 213 impact the goals and strategies the Administration articulated in the President's August 2011 plan for how the Federal Government will support and help empower American communities and their local partners to prevent violent extremism?

Response: DHS's approach to counter violent extremism (CVE) includes integrating a better understanding of the dynamics of violent extremism and the risk it poses to the United States, and raising broader awareness on the issue across the Department. Instead of treating violent extremism as a separate function of these operational entities, the Department's approach seeks to leverage the strength and capabilities of each components core capabilities in its efforts to deal with this issue.

By doing so, DHS leverages its existing programs, resources, and relationships for direct and indirect CVE purposes. DHS has established the Countering Violent Extremism Working Group (CVEWG) to better coordinate the Department's operational and programmatic efforts to counter violent extremism. John Cohen, Senior Advisor to the Secretary, is responsible for coordinating the Department's CVE efforts.

67123.646

Question#:	6
Topic:	oversight board
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The former Chairmen of the 9/11 Commission released a report on August 31, 2011, listing nine of their recommendations that remain unfinished, including the absence of a functioning Privacy and Civil Liberties Oversight Board. In April, I joined Senators Lieberman and Collins in a letter to the President asking that he nominate a full slate of members so the Board could operate. To date, I have not received a response. What is the status of the Privacy and Civil Liberties Oversight Board being formed?

Response: The Department of Homeland Security is not involved with establishing the Privacy and Civil Liberties Oversight Board. We understand that the President now has nominated a full slate of members for the Board. When it is in place, the Department, through the Privacy Office and Office for Civil Rights and Civil Liberties, looks forward to consulting with the Board to further ensure the Department's activities preserve privacy, civil rights, and civil liberties to the greatest extent possible.

67123.647

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Mark L. Pryor

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

Question#:	7
Topic:	threat level
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: The threat level for the 10th anniversary of September 11th was raised.

Can you address what prompted the heightened alert and what considerations go into raising the threat level?

How did agencies work together at all levels of government to ensure that the American people were as safe as possible on the anniversary of September 11th?

Response: In April 2011, DHS replaced the color-coded alert system, created shortly after the 9/11 attacks, with the new National Terrorism Advisory System (NTAS)—a robust terrorism advisory system that provides timely information to the public and the private sector, as well as to state, local, and tribal governments about credible terrorist threats and recommended security measures.

DHS did ***not*** issue a National Terrorism Advisory System (NTAS) Alert around the anniversary of 9/11.

Under NTAS, DHS coordinates with other Federal entities to issue detailed alerts to the public when the Federal Government receives information about a credible terrorist threat.

In close collaboration with other Federal Departments and Agencies—including the Federal Bureau of Investigation—and the Department's state, local, and private sector partners, DHS coordinated its activities around the 10th anniversary of September 11, 2011, around four areas:

1) Intelligence & Information Sharing/Understanding & Monitoring the Threat;
2) Operational Activities – Prevention/Protection Measures;
3) Crisis Management; and
4) Stakeholder Outreach & Public Awareness including the "If You See Something, Say Something" Campaign.

Further details are available in a classified setting.

67123.648

Question#:	8
Topic:	budget
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: Keeping in mind the current fiscal situation, what are the future challenges for DHS? Have you identified areas in DHS that could sustain spending cuts in DHS? What missions may be the most endangered by budget constraints?

Response: Our investments over the past ten years have directly resulted in an improved capacity to detect, protect, prevent, respond, and recover from terrorist attacks. Our communities are safer directly because of these investments. Acknowledging current budget challenges, we must continue to implement initiatives to increase fiscal responsibility in order to meet our mission and support frontline operations.

The Department has implemented a variety of initiatives to cut costs, share resources across Components, and consolidate and streamline operations wherever possible. Our recent budget submissions have redirected hundreds of millions in base resources from administrative and mission support areas, including contracts, personnel (through attrition), information technology, travel, personnel moves, overtime, directed purchasing, professional services, and vehicle management. Through the Department-wide Efficiency Review, which began in 2009, as well as other cost-saving initiatives, the Department of Homeland Security (DHS) has identified over $3 billion in cost avoidances and reductions, and redeployed those funds to mission-critical initiatives across the Department.

At the same time, the Department has challenged its workforce to fundamentally rethink how it does business – from the largest to smallest investments. In 2011, DHS conducted its first-ever formal base budget review for FY 2013, looking at all aspects of the Department's budget to find savings within our current resources and to better align those with operational needs. Through its annual "Think Efficiency Campaign," DHS solicited employee input on creative cost-saving measures and will implement six new employee-generated initiatives in early 2012.

By focusing on efficiencies and cost-savings wherever they can be achieved, we have been able to maximize our resources and provide the best support possible for our frontline operations.

With these efforts in mind, we must continue to look for ways to effectively meet our mission under the constraints of the changing fiscal environment at a time when the demands on our department and the entire homeland security enterprise have never been greater.

67123.649

Question#:	9
Topic:	death
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: I think everyone would agree that Americans and people around the globe feel safer without the threat of Osama bin Laden.

Now that he is no longer a threat, how is the Department addressing the threat of bin Laden supporters who seek revenge?

Does his death change anything for the Department?

Response: Al-Qa'ida has been significantly degraded as a result of U.S. counterterrorism operations and there is no specific or credible intelligence that al-Qa'ida or its affiliates are plotting imminent attacks in the United States at this time. However, the group continues to pose a serious threat to U.S. interests, including to the homeland. We remain at a heightened state of vigilance and security measures are in place to detect and prevent plots against the United States should they emerge.

Our security posture, which always includes a number of measures both seen and unseen, will continue to adapt appropriately to protect the American people from an evolving threat picture.

Homeland security is a shared responsibility, and everyone has a role to play. Even as DHS continues to work with partners both at home and abroad, we remind our federal, state, local, tribal and territorial partners and the public to remain vigilant and to report any suspicious activity to local law enforcement authorities.

67123.650

Question#:	10
Topic:	resilience
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: Under the National Strategy for Counterterrorism, one of the core principles guiding our counterterrorism efforts is "building a culture of resilience." The goal of this principle reaches a step beyond preparedness and focuses on promoting an individual and community sense of being able to recover and rebuild from catastrophic events.

How do you envision promoting this principle of resilience?

Response: The Department of Homeland Security (DHS) is incorporating homeland security and counterterrorism capabilities into our day to day efforts to protect our communities from violence. We are building the capacity to understand threats, put threats into a local context, and draw from research analysis to recognized indicators and encourage awareness and vigilance by members of the public. This includes, promoting the National Suspicious Activity Reporting (SAR) Initiative to Fusion Centers and State and Local law enforcement. It also includes expansion of the "If You See Something Say Something™" Campaign.

DHS's primary framework for systematically building a culture of resilience and assessing progress toward this goal is through response to Presidential Policy Directive 8 (PPD-8). The National Preparedness Goal outlines and integrates the capabilities and performance measures for resilience across all mission areas. The National Preparedness System will include integration of planning frameworks, as well as recommendations and guidance for implementation. The National Preparedness System will build on current assessments through the Quadrennial Homeland Security Review (QHSR) and will include a comprehensive approach to methodology and assessment. The expansion of a coordinated, comprehensive campaign to build and sustain preparedness, including "public outreach and community-based and private sector programs to enhance national resilience..." is a priority for PPD-8 implementation.

DHS believes that well-informed and equipped families, communities, and local institutions represent a critical defense against threats and hazards—natural and man-made—and that public resilience is key to national resilience. In order to establish resilient communities, there must be active and trusting partnerships built among communities, including Federal, state, local, and tribal governments. DHS promotes resiliency to communities via public awareness campaigns, such as Ready.gov, for preparedness. To further engage the public in homeland security, the Department also launched the "If You See Something, Say Something" campaign in July 2010. Used with permission of the New York Metropolitan Transportation Authority (MTA), the "If You

67123.651

Question#:	10
Topic:	resilience
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

See Something, Say Something ™" campaign is run out of the Office of Public Affairs and is coordinated with components across the Department.

The Department has worked to integrate resiliency into its mission and promote it through a coordinated whole-of-government approach. For counterterrorism, law enforcement officers are trained on improved engagement with communities and community-oriented policing, grievance, and outreach efforts. The Federal Emergency Management Agency (FEMA) promotes programs such as local Community Emergency Response Teams that train the public to respond to emergency situations in their communities, give critical support to first responders, provide immediate assistance to victims, and organize spontaneous volunteers at a disaster site. FEMA's community engagement and local Citizen Corps Councils promote sustained dialogues with Government to include community leaders in planning efforts, to educate the public on risks, to empower the community with knowledge on how to respond to disasters of all kinds, and to train and integrate non-governmental resources. Current initiatives focus on working with young Americans and groups that are traditionally not engaged in order to integrate the public into community resilience planning and to bolster the relationships and partnerships that are essential for creating resilient communities.

The Department's National Protection and Programs Directorate (NPPD) also works closely with state, local, tribal, and private sector partners to promote resilience initiatives across the Nation's critical infrastructure sectors. Additionally, NPPD leads the Federal Government's efforts to advance resilience initiatives in cybersecurity. Recent resilience programs in the cyber arena include public outreach and awareness campaigns such as National Cybersecurity Awareness Month and "Stop.Think.Connect."

There is also a Headquarters driven element on resilience. Known as the Resilience Integration Team (RIT), this group is comprised of subject matter experts from across the Department. RIT is developing cross-component initiatives to build a national culture of resilience. One initiative entails the creation of a National Resilience Award which was announced in New York City during National Preparedness Month 2011. The Award will be given out annually on 9/11 by the Secretary of Homeland Security to an individual, community or organization exhibiting leadership in resilience.

The Resilience STAR initiative is another cross-component initiative that is in the process of being developed by the RIT. Similar to Energy STAR, Resilience STAR provides a voluntary designation for homes and buildings with design features that enhance resilience to disasters. The initial phases of the initiative focus on incentivizing stakeholders to build and retrofit private residences and commercial facilities that better

67123.652

Question#:	10
Topic:	resilience
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

withstand disruption. The program will also include critical infrastructure such as transportation sector infrastructure.

Question: How do you measure resilience?

Response: PPD-8 performance metrics will build on and augment metrics currently in place through the QHSR and program-level evaluation. QHSR measures focus on individual preparedness, mitigation, and recovery, such as:

- Percent of households surveyed reporting they have taken steps to be prepared in the event of a disaster.
- Percent of households surveyed reporting they have taken steps to mitigate damage to property and protect themselves in the event of a disaster.

As part of FEMA's National Disaster Recovery Framework, FEMA emphasizes that post-disaster community planning is key and that the planning process provides the benchmark to measure the affected community's progress toward a successful outcome. Communities impacted by disasters should develop a process for optimally managing their recovery efforts and resources.

67123.653

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Claire McCaskill

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

Question#:	11
Topic:	databases
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: A lot of the testimony given at this hearing related to the sharing of information with your counterparts at the FBI and the National Counterterrorism Center (NCTC). Yet, within DHS and its components, information sharing and the interoperability of databases across the components and the department is poor or non-existent.

Can you describe which DHS databases are compatible with those of other agencies? Are they also compatible between DHS and its components?

Do you believe that vital information from the components are reaching the appropriate officials at the local level? If so, what is the process and how are you measuring effective information dissemination?

Response: DHS has made progress in ensuring the interoperability of databases across components to protect the homeland, facilitate legitimate commerce, and combat fraud. As part of this vision, DHS adopted a "One DHS" policy for information sharing among components.

To enable this capability, DHS focused its interoperability efforts in two areas. First, DHS provided a central point of integration for information from multiple sources to its front line operators, by developing products such as the Custom and Border Protection (CBP) Federated Person Query that integrates information from up to 16 databases used by Border Patrol Agents and the U.S. Citizenship and Immigration Services (USCIS) Person Centric Query System that integrates information from 21 databases used by Immigration Benefit Adjudicators. Second, DHS has four primary data aggregation systems that are used across the Department such as CPB's Automated Targeting System, the Transportation Security Administration's (TSA) Crew Vetting Platform, the Immigration and Customs Enforcement Pattern Analysis and Information Collection System (ICEPIC), and United States Visitor and Immigrant Status Indicator Technology

67123.654

Question#:	11
Topic:	databases
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

(US-VISIT) Program's Arrival and Departure Information System (ADIS). Additionally, DHS personnel may access approximately 25 additional high value databases through either integrated access or data aggregation systems. Because of these efforts, DHS personnel are better able to access and share information needed to perform their duties. Additionally, based on a comprehensive overstay review conducted this summer, DHS is leveraging data processing toolsets, integrating data sources and automating the feeds between databases to establish a enhanced biographic exit capability, which further can serve as the foundation for a biometric exit solution.

DHS continues to work with the National Security Staff (NSS), key departments and agencies, and other external partners to provide and receive federated access to government-held data, as appropriate, in a continuous, consistent, and high quality manner. For example, in late 2011, DHS screening systems, like Secure Flight, will begin receiving real time feeds from the Terrorist Screening Database managed by the FBI's Terrorist Screening Center.

Nevertheless, the U.S. Government faces both technical and non-technical challenges around the design and implementation of comprehensive data aggregation systems, including legal and policy requirements for data discovery, access, ingest, use, and retention of person-centric data. As recently as September 28, 2011, the first-ever 'Whole of Government Data Aggregation Summit' identified numerous and complex legal, technical, policy and procedural challenges associated with the distribution of mission critical data across existing information sharing architectures. As part of DHS's resolve to find solutions to these challenges, the Department is the executive agent for the NSS's Information Sharing and Access Interagency Policy Committee- (IPC) / Information Sharing Environment Program Manager- (PM ISE) sponsored pilots that will help to optimize the standardized format and distribution methods for sharing data with external agencies such as the FBI and the National Counterterrorism Center (NCTC). This work is based on best practices such as the use of the National Information Exchange Model (NIEM).

DHS has worked closely with NCTC and FBI to improve the quality and relevancy of intelligence products disseminated to State, local, tribal, and territorial officials. Furthermore, DHS has worked to build analytic capacities at the grass-roots level by supporting regional fusion centers so that national intelligence can be viewed within the context of local conditions, thereby allowing state, local and tribal authorities to better assess the risk to their communities. Third, the DOJ-led Nationwide Suspicious Activity Reporting (SAR) Initiative has helped to ensure that suspicious activity is reported to Fusion Centers, and that Fusion Center directors are adequately trained to pass threat-related information to JTTFs for further investigation.

67123.655

Question#:	12
Topic:	priorities
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Since 9/11, Homeland Security related spending has accounted for an increasing share of discretionary spending. As the 9/11 Commission Recommendations Progress Report 2011 stated, "the demands on DHS have never been greater, the current fiscal climate requires the Department to continue to maximize every security dollar".

In light of the inevitable fiscal restraints on discretionary spending, what are the three top priorities for the Department in the upcoming year?

Response: The Department continues to focus efforts across its five mission areas as identified in the Quadrennial Homeland Security Review: preventing terrorism, securing our borders, enforcing immigration laws, cybersecurity and disaster response and recovery.

Question: How will they strengthen DHS's homeland security effort?

Response: Protecting the United States from terrorism is the cornerstone of homeland security. DHS's counterterrorism responsibilities focus on three goals: preventing terrorist attacks; preventing the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear materials and capabilities within the United States; and reducing the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards.

DHS secures the Nation's air, land, and sea borders to prevent illegal activity while facilitating lawful travel and trade. The Department's border security and management efforts focus on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding and streamlining lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations.

DHS is focused on smart and effective enforcement of U.S. immigration laws while streamlining and facilitating the legal immigration process. The Department has fundamentally reformed immigration enforcement, focusing on identifying and removing criminal aliens who pose a threat to public safety and targeting employers who knowingly and repeatedly break the law.

DHS is the Federal Government lead agency for securing civilian government computer systems, and works with industry and State, local, tribal and territorial governments to secure critical infrastructure and information systems. DHS analyzes and mitigates cyber

67123.656

Question#:	12
Topic:	priorities
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

threats and vulnerabilities; distributes threat warnings; and coordinates the response to cyber incidents to ensure that our computers, networks, and cyber systems remain safe.

DHS provides the coordinated, comprehensive Federal response in the event of a terrorist attack, natural disaster, or other large-scale emergency while working with Federal, State, local, and private sector partners to ensure a swift and effective recovery effort. The Department's efforts to build a ready and resilient Nation include fostering a community-oriented approach, bolstering information sharing, improving the capability to plan, and providing grants and training to our homeland security and law enforcement partners.

Question: Where can you consolidate, eliminate or restructure other programs in order to accomplish these priorities without incurring extra costs?

Response: Reflecting on the current economic environment, we are preserving essential frontline operations and bolstering our operational strength by decreasing administration and overhead costs, including the overall budget for the Office of the Secretary and Executive Management. All DHS Components identified reductions associated with the Secretary's Efficiency Review (ER) initiatives that have been underway for nearly three years, as well as administrative savings to strengthen mission critical activities. Through the ER and other cost-saving initiatives, DHS has identified over $3 billion in cost avoidances and reductions.

Savings were accomplished through efficiencies in acquisition, asset and real property management as well as employee vetting/credentialing, hiring and information technology, and administrative cost reductions. This last category includes reducing or eliminating professional services contracts, printing, supplies and materials, travel and training.

67123.657

Question#:	13
Topic:	strategic needs
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, the September 7, 2011, GAO report titled "Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years After 9/11" recognized the strides DHS has made in protecting the nation but also asserted that DHS has yet to reach its full potential. The report specifically pointed out that limited strategic and program planning by DHS has contributed to programs not meeting strategic needs in an efficient manner. Can you provide specific examples of changes made at DHS to address this concern raised by GAO? Have those same changes been made at the component level?

Response: Perhaps the best way to see the specific examples of changes made at DHS addressing strategic and programmatic planning is to apply a snap-shot of today's security architecture regarding what did, and did not exist when the terrorist attacks of 9/11 occurred.

Expanding Information Sharing

Through close partnerships with federal, state and local governments, community-based organizations, and private sector partners, DHS works to ensure that resources and information are available to state and local law enforcement, giving those on the frontlines the tools they need to protect local communities.

Under the National Terrorism Advisory System (NTAS), DHS coordinates with other federal entities to issue detailed alerts to the public when the federal government receives information about a specific, credible terrorist threat to the United States.

DHS works closely with its partners across the federal government on various information sharing initiatives to support law enforcement operations and protect the country from terrorists and other threats. DHS also has expanded its work with Tribal governments and law enforcement across the nation.

Today, the DHS Visa Security Program deploys trained special agents to high-risk posts around the world to identify potential terrorist and criminal threats before they ever reach the United States. ICE agents assigned to Visa Security Units overseas liaise with local law enforcement and share information with the U.S. Department of State in day-to-day operations as part of a layered approach to national security.

Developing and Implementing Risk-based Transportation Security Strategies

67123.658

Question#:	13
Topic:	strategic needs
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

DHS focuses on intelligence-driven security across all modes of transportation to enhance the security of the Global Supply Chain. We made significant advances in risk-based security, including conducting baseline security assessments across aviation, maritime, and surface transportation sectors; historic global aviation standards; advanced passenger and cargo information; and enhanced information sharing with international and private sector partners. DHS also focused on strengthening maritime transportation security through a risk- and technology-based approach by evaluating vulnerabilities and mitigating threats across all potential pathways.

Strengthening Airline Passenger Pre-screening and Targeting Terrorist Travel

With support from international partners and the aviation industry, DHS has implemented pre-departure screening programs for flights bound for the United States as well as enhanced security measures to strengthen the safety and security of all passengers. DHS has worked closely with the intelligence and law enforcement communities to develop new mechanisms that identify high-risk travelers prior to departure. In fiscal year 2010 (FY 2010), DHS identified more than 1,500 passengers on watchlists who had booked international flights. Through its law enforcement function, the U.S. Immigration and Customs Enforcement's (ICE) Visa Security Program serves an important role in recognizing potential security threats in the visa process.

Enhancing Screening for Explosives

Prior to 9/11, limited federal security requirements existed for cargo or baggage screening. The presence of frontline security personnel at the passenger checkpoints and new technologies has enhanced security. In addition, there has been a concomitant increase in regulation and security for air cargo.

As noted earlier, prior to 9/11, limited federal security requirements existed for air cargo screening. In December 2010, the Transportation Security Administration (TSA) implemented requirements for 100 percent screening of high-risk cargo on international passenger and cargo flights bound for the United States. As part of this effort, TSA is working with industry to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process.

Protecting Critical Infrastructure

Since FY 2006, DHS has provided more than $3.6 billion in grant funding through the Port Security, Transit Security and Buffer Zone Protection grant programs to protect

67123.659

Question#:	13
Topic:	strategic needs
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

critical infrastructure from terrorism. These risk based security grants support security plans, facility security upgrades, training, exercises, law enforcement anti-terrorism operations, and capital projects for risk mitigation of high threat infrastructure.

DHS also developed an annual National Risk Profile that provides a multi-hazard assessment of risks facing critical infrastructure, including terrorist threats, cyber risks, and natural disasters.

Since 2007, DHS has implemented the Chemical Facility Anti-Terrorism Standards (CFATS) to regulate security at high-risk chemical facilities. Additionally, the DHS Science and Technology (S&T) Directorate also conducts research and development to create new technologies to enhance critical infrastructure security. Since 9/11, DHS has worked to transform and strengthen interoperable communications across the country.

Bolstering the* Security *of U.S. Borders and Identification Documents

At the same time, DHS has made critical security improvements along the Northern and Southwest borders, investing in additional U.S. Border Patrol agents, technology, and infrastructure while also strengthening efforts to increase the security of the nation's maritime borders.

DHS continues to invest in personnel, technology, and infrastructure, and to strengthen cooperation with federal, state/provincial, tribal, and private sector partners on both sides of the border. DHS has made important security improvements along the Northern border, investing in additional U.S. Border Patrol agents, technology, and infrastructure. The U.S. Coast Guard's (USCG) overarching strategy is to increase maritime border security through a layered security system that begins beyond the country's physical borders. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases, a percentage that is steadily rising as new technology and infrastructure are deployed along the borders. Through the Visa Security Program, which did not exist on 9/11, ICE, with State Department concurrence, deploys trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States. The ICE-led Border Enforcement Security Task Force (BEST) initiative currently has 11 established BESTs along the Southwest Border, which leverage Federal, State, local, tribal and foreign law enforcement and intelligence resources in an effort to identify, disrupt, and dismantle organizations that seek to exploit vulnerabilities along the U.S. borders and threaten the overall safety and security of the American public.

U.S. Citizenship and Immigration Services has embedded Fraud Detection and National Security officers in eight other government agencies to increase information sharing and collaboration efforts that enhance law enforcement and intelligence operations. The DHS Privacy Office partners with every DHS component to assess policies, programs, systems, technologies, and rulemakings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information.

67123.660

Question#:	14
Topic:	S and T
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Within DHS there is an office dedicated to science and technology (S & T) which, some argue, has performed below expectations. This office was created with the vision of innovation and integration across components as well as working with DOD and private industry. Instead, products are leaving the lab with minimal testing in "actual settings." There is no coordination within the department on input received from the component using the product. These products, if functional, would supplement the incredible work being performed by your personnel. Instead, once implementation began most projects are being scrapped. Below are some examples of projects that that were eventually ended. For each project, please provide: the total investment made in the project; project purpose; and a justification for why the projects were abandoned.

Please explain what processes, procedures and verification methods have been adopted by the Science and Technology Directorate to avoid such phenomenal losses of money in the future.

Response: The Department is in the process of establishing and implementing the Integrated Investment Life Cycle Model (IILCM). As part of the IILCM model a Capabilities Requirements Council, made up of senior Department and Component leaders, evaluates requirements to ensure strategic alignment. Once requirements are validated and a program is established, the Department's Investment Review Board (IRB), provides program oversight at specific milestones in the investment lifecycle. Between these milestones, Executive Steering Committees (ESC) are established to provide consistent and effective governance of the programs, and where deviations from approved plans occur, they are identified early allowing for corrective actions to be taken.

As part of the IICLM, S&T plays a role in the operational test and evaluation of technologies, which will help determine whether technology is ready before reaching the field.

Question: Cargo Advanced Automated Radiography System

Response: The Domestic Nuclear Detection Office (DNDO) Cargo Advanced Automated Radiography System (CAARS) program sought to develop and demonstrate non-intrusive inspection technology that could automatically identify dense materials that could be used to shield special nuclear and radiological threat materials in vehicles and containers at ports of entry. In 2007, DNDO recognized that the CAARS technology was not as mature as originally anticipated. Accordingly, DNDO scaled the program back

67123.661

Question#:	14
Topic:	S and T
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

from an acquisition program to a research and development program. Following the course correction, the CAARS program was conducted as a research and development program designed to demonstrate the potential future capability of the technology through the development and evaluation of prototype systems. The CAARS research and development program reached its conclusion at the end of Fiscal Year 2010. DNDO is migrating useful technologies developed through the CAARS program to advance other research and development efforts and will continue testing commercially available non-intrusive imaging systems.

Question: EINSTEIN 2

Response: The EINSTEIN 2 program is a system that was developed and is currently maintained by the National Protection and Program Directorate's Office of Cybersecurity and Communications, which provides an intrusion detection capability that is currently operational at 16 of 19 Federal Executive Branch Civilian agencies, which serve as Trusted Internet Connection (TIC) Access Providers to improve Federal networks' cybersecurity posture. All other agencies are or will be covered by EINSTEIN 2 through the Managed Trusted Internet Protocol Services, a General Services Administration vehicle for purchasing TICs as a managed service. EINSTEIN 2 is one facet of the overall National Cybersecurity Protection System, which is an integrated intrusion detection, analytics, information sharing, and intrusion prevention system that utilizes hardware, software, and other components to support Department of Homeland Security (DHS) responsibilities within the Comprehensive National Cybersecurity Initiative mission. The performance of the program is routinely reviewed by a DHS review board.

Question: Puffer Machines for Airport Security

Response: The Trace Portals (puffer machines) were developed to screen people for trace explosives residue at the airport checkpoint. The Science and Technology Directorate's Transportation Security Laboratory was involved in developmental and laboratory testing of the puffer portals. TSA determined that Trace Portals did not meet the requirements for operational suitability due to frequent maintenance issues. TSA also determined that more reliable and effective screening technologies, such as millimeter wave and backscatter Advanced Imaging Technology, have become available since the Trace Portals were first introduced. For these reasons, TSA decided to phase out this technology. In 2009, TSA opened the TSA Systems Integration Facility (TSIF), a state-of-the-art testing facility at Ronald Reagan Washington National Airport. The TSIF improves testing and evaluation of new technologies by allowing TSA to examine technologies and screening procedures in a realistic airport environment.

67123.662

Question#:	14
Topic:	S and T
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Secure Border Initiative Network

Response: In 2010, Secretary Napolitano directed an independent, quantitative assessment of the SBInet program, which combined the input of U.S. Border Patrol agents on the front lines with the Department's leading science and technology experts. This assessment made clear that SBI*net* could not meet its original objective of providing a one-size-fits-all border security technology solution. As a result, earlier this year, CBP began the process of redirecting SBI*net* resources to other, proven technologies – tailored to each border region – to better meet the operational needs of the Border Patrol. This new border security technology plan is providing faster deployment of technology, better coverage, and a more effective balance between cost and capability.

67123.663

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Susan M. Collins

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

Question#:	15
Topic:	fusion centers - 2
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: What is being done to ensure that these JTTFs and fusion centers have good relationships and that competition between the two organizations does not prevent much needed information sharing?

What are some specific examples of how fusion centers are contributing to the homeland security mission by developing new cases, identifying new threats, and how their relationships with state and locals have yielded better analysis or response to emergencies and events?

It is also my understanding that I&A has implemented a program of analysis to measure quality of its analytic products and customer satisfaction – are fusion centers participating in this program as well, if not, why not?

What is your assessment of how State and local partners are benefiting from the current information sharing environment?

How has state and local fusion centers added value to the intelligence process at the national level?

What programs have you instituted to measure this progress?

Response: The national security enterprise must reach beyond the capabilities of the federal government and national Intelligence Community to identify and warn of impending plots that could impact the homeland, particularly when the individuals responsible for the threats operate within the United States and do not travel or communicate with others overseas. Together, Fusion Centers and Joint Terrorism Task Forces (JTTFs) make up part of a cohesive national effort intended to rapidly identify and investigate emerging threats. Establishing this capability has directly impacted our capacity to protect our communities from violence. DHS has worked closely with the

67123.664

Question#:	15
Topic:	fusion centers - 2
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

FBI to ensure that state and major urban area fusion centers and the JTTFs serve distinct, but complementary, roles in securing the Homeland.

Fusion centers are owned and operated by State and local entities and, as described in the *National Strategy for Information Sharing*, serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information among Federal and State, local, tribal, and territorial partners. Fusion centers receive threat information from the federal government; analyze that information in the context of their local environment; disseminate relevant products and information to local customers to assist in identifying and addressing immediate and emerging threats; and gather tips, leads, and suspicious activity reporting (SAR) from local agencies and the public. Beyond serving as a focal point for information sharing, fusion centers add significant value to their customers by providing a State and local context to national intelligence. Fusion centers provide the Federal government with critical State and local information and subject matter expertise – enabling the effective communication of locally generated threat-related information to the federal government. Furthermore, they produce actionable intelligence, which can aid other law enforcement organizations, including the JTTFs, in their investigative operations.

JTTFs are multi-jurisdictional task forces established to conduct terrorism-related investigations and to collect foreign intelligence domestically. JTTFs focus exclusively on terrorism-related issues, and conduct terrorism investigations with local, regional, national, and international implications. JTTFs focus their investigations on observed threat activity or actors who meet the thresholds established in accordance with the Attorney General's *Guidelines for Domestic FBI Operations* to initiate assessments or investigations.

As partners in the national homeland security enterprise, fusion centers and JTTFs collaborate to add value to their respective primary missions: fusion centers analyze and share intelligence, while JTTFs conduct investigations.

Fusion centers have provided invaluable information on a number of the nation's most significant homeland security threats including the attempted Times Square Bombing, Najibullah Zazi plot against the New York Subway and 9/11 Anniversary events. Beyond the significant support to counterterrorism efforts, fusion centers provide important and timely analysis to support an all-crimes approach to protecting communities, on issues ranging from automobile and metal thefts to drug trafficking issues.

67123.665

Question#:	15
Topic:	fusion centers - 2
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

The following are some more recent examples of fusion center contributions to the homeland security mission:

- In June 2011, the Colorado Information Analysis Center (CIAC) assisted the JTTF and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) with the creation and distribution of a "Be On Look Out" (BOLO) bulletin to all local law enforcement agencies regarding a vehicle suspected of being associated with two improvised explosive devices detonated at a Borders bookstore. Less than 15 minutes after sending this information, the CIAC received vital information from a State Trooper/Terrorism Liaison Officer (TLO). Approximately twenty-four hours earlier, an individual matching the description in the BOLO was taken into custody, and this information was passed to the CIAC and individual FBI JTTF.

- The Pennsylvania Criminal Intelligence Center (PaCIC) provided information regarding the abduction and rape of a woman, which included a description of the suspect as well as his Maine license plate number. A fusion center analyst at the PaCIC provided the information to the Maine Intelligence Analysis Center along with details on the case. Based on this coordination, the Maine State Police determined the suspect had fled the United States for Canada. Working with the Royal Canadian Mounted Police in New Brunswick, Canada, the suspect was found and arrested on charges of kidnapping and rape.

- The Arizona Counter Terrorism Information Center supported a five-month investigation led by a tribal partner, the Tohono O'odham Nation (TON) Police Department and the Bureau of Indian Affairs Division of Drug Enforcement. This investigation led to the arrest of 10 suspects and the apprehension of weapons, cash, vehicles, cocaine, marijuana, and ecstasy in May 2010 – the largest drug enforcement operation in TON history. The investigation marked a key opportunity to collaborate with tribal partners and opened information sharing initiatives between several other agencies, including the FBI, ATF, and other police departments in the area.

Fusion Center analysts also collaborate with analysts at DHS I&A to develop products of interest to multiple fusion centers and the intelligence community as a whole. Access to and analysis of national threat information enables State and local partners to understand local implications and direct resources accordingly. Working cooperatively with DHS also enables State and local law enforcement agencies an opportunity to leverage the spectrum of specialized skills and assets that DHS possesses, resources to which State and local law enforcement would not otherwise have access. State and local partners also have an opportunity to inform national leadership on significant trends in criminal activity and the activities of violent extremists of which senior leadership in the intelligence community and policy makers are often not yet aware.

67123.666

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Ron Johnson

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

Question#:	16
Topic:	Budget levels
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Question: The creation of the Department of Homeland Security (DHS) consolidated 22 different agencies into one Department. The budget of DHS has risen from approximately $22 billion to approximately $56 billion since fiscal year (FY) 2002, an increase of nearly threefold.

Please detail the total actual or estimated FY budget levels for DHS from FY 2003-2011.

For FY 2002, please provide actual budget levels for the 22 legacy components of the Department of Homeland Security. Where possible, please provide numbers that align with current Department of Homeland Security components (i.e., Federal Emergency Management Agency, Immigration and Naturalization Service). Understanding that some components existed in different forms prior to the creation of the Department, please attempt to estimate the cost of performing those activities in Fiscal Year 2002 (i.e., the Transportation Security Administration did not exist in its current form, however, please provide an estimate of what was spent on performing the functions that TSA currently performs today). Please also include associated FY 2002 full time employee (FTE) numbers with each fiscal allocation.

How does the Department of Homeland Security classify its employees in terms of those that are (a) administrative or managerial in duties and (b) those that have operational responsibilities? Please provide the current FTE levels for each of these types of employees within the Department of Homeland Security.

Please identify which offices or portions of offices in DHS are considered to be part of the administrative or managerial capacity of the department. This should include headquarters level offices or portions of offices (ex. DHS Public Affairs Office) as well as component level offices or portions of offices (ex. TSA Strategic Communications and Public Affairs) that perform administrative or managerial functions. Please provide fiscal year 2011 funding levels for these offices or portions of offices and current FTEs.

Please detail the headcount of FTEs of the Department of Homeland Security by component for

67123.667

Question#:	16
Topic:	Budget levels
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

every fiscal year since the inception of DHS.

Response: The Department was stood up in early 2003, but did not have a consolidated appropriated budget until FY 2004 (enacted October 1, 2003). Consequently, numbers provided for FY 2003 in Table 1 are estimates of the level of funding appropriated to legacy agencies for component parts that were later transferred to DHS.

The following table shows the appropriated levels in FY 2002 for the legacy Components of DHS, where known. The successive table shows an estimate, compiled in February 2003, of the FY 2002 funding levels of legacy DHS Components, as if DHS existed in FY 2002.

Function/Organization	Former Agency	FY 2002 Appropriated Funding (in millions)[1]	Source	Current Component
Plum Island Animal Disease Center	Dept Agriculture	$3.7	H.R. 107-275	S&T
National Infrastructure Simulation and Analysis Center	Dept of Energy	$19.3	GAO Report 03-250	NPPD
Federal Law Enforcement Training Center	Dept of Treasury	$139.1	H.R. 107-253	FLETC
Federal Protective Service[2]	GSA	$0	GAO Report 03-8	NPPD
Secret Service	Dept of Treasury	$924.2	H.R. 107-253	USSS
Transportation Security Administration	Dept of Transportation	$1,403.8	H.R. 107-308	TSA
Customs Service	Dept of Treasury	$2,688.1	H.R. 107-253	CBP, ICE
Federal Emergency Management Agency	FEMA	$3,058.9	H.R. 107-272	FEMA
Immigration and Naturalization Service	Dept of Justice	$3,499.9	H.R. 107-278	CBP, ICE, USCIS
Coast Guard	Dept of Transportation	$5,030.5	H.R. 107-308	USCG
Agriculture Quarantine and Inspection Program	Dept Agriculture	N/A	N/A	CBP
Critical Infrastructure Assurance Office	Dept of Commerce	N/A	N/A	NPPD

67123.668

Question#:	16
Topic:	Budget levels
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Function/Organization	Former Agency	FY 2002 Appropriated Funding (in millions)[1]	Source	Current Component
Domestic Emergency Support Team	Dept of Justice - FBI	N/A	N/A	FEMA
Federal Computer Incident Response Center	GSA	N/A	N/A	NPPD
National Communications System	Dept of Defense	N/A	N/A	NPPD
National Domestic Preparedness Office	Dept of Justice - FBI	N/A	N/A	FEMA
National Infrastructure Protection Center	Dept of Justice - FBI	N/A	N/A	NPPD
Office for Domestic Preparedness	Dept of Justice	N/A	N/A	FEMA

Notes:
[1] Program funding level data are not currently available. Dollars in millions.
[2] FPS is fee funded. It had an operating level of $362 million in FY 2012.

As shown in the table below, which was compiled in January 2003, the funding for legacy DHS organizations in FY 2002 is estimated to be $36.4 billion, of which $22.1 billion was initially appropriated and $14.3 billion was provided in supplemental funding, in response to the events of 9/11. Compared with the FY 2011 budget of $55.1 billion, DHS appropriations have increased by about 50% above the budgets of its legacy agencies in FY 2002 in order to address evolving threats and support frontline security operations. This estimate was made with limited data provided by the parent organizations of the legacy agencies and may not represent complete funding information.

Funding by Account
As if DHS Existed in FY 2002
(budget authority in millions of dollars)

	2002 Enacted	2002 Supplemental	Total
Border and Transportation Security			
U.S. Customs and Border Protection	5,057	870	5,927
U.S. Immigration and Customs Enforcement	2,394	179	2,573
Transportation Security Administration	1,242	2,435	3,677

67123.669

Question#:	16
Topic:	Budget levels
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Funding by Account
As if DHS Existed in FY 2002
(budget authority in millions of dollars)

	2002 Enacted	2002 Supplemental	Total
Federal Law Enforcement Training Center	137	31	168
Office of Domestic Preparedness	260	635	895
Customs Abandoned Goods	6	---	6
Total, Border and Transportation Security	**9,096**	**4,150**	**13,246**
Emergency Preparedness and Response			
Operating Expenses	734	1,365	2,099
Grant Programs	20	---	20
Disaster Relief	2,093	8,038	10,131
Disaster Assistance Direct Loan Program Account	1	---	1
Emergency Food and Shelter[1]	140	---	140
National Flood Insurance Fund	1,536	---	1,536
Flood Map Modernization Fund	32	---	32
Total, Emergency Preparedness and Response	**4,556**	**9,403**	**13,959**
Science and Technology	**90**	**77**	**167**
Information Analysis and Infrastructure Protection	**117**	**36**	**153**
U.S. Coast Guard			
Operating Expenses	3,434	398	3,832
Capital Acquisitions	647	66	713
Retired Pay	876	---	876
Boat Safety	64	---	64
Trust Fund Share of Expenses[2]	48	---	48
Oil Spill Recovery	101[3]	---	101
Miscellaneous Trust Revolving Funds[4]	9	---	9
Total, U.S. Coast Guard	**5,179**	**464**	**5,643**
U.S. Citizenship and Immigration Services	**1,567**	**37**	**1,604**
U.S. Secret Service			
Operating Expenses	1,114	105	1,219
Capital Acquisitions	3	---	3
Total, U.S. Secret Service	**1,117**	**105**	**1,222**
Departmental Management			
Departmental Operations	225	---	225
Counterterrorism Fund	40	---	40

67123.670

Question#:	16
Topic:	Budget levels
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Funding by Account
As if DHS Existed in FY 2002
(budget authority in millions of dollars)

	2002 Enacted	2002 Supplemental	Total
Department-wide technology investments	87	---	87
Total, Departmental Management	**352**	**---**	**352**
Office of the Inspector General	**47**	**---**	**47**
Total, Department of Homeland Security Funding	**22,121**	**14,272**	**36,393**

[1] Proposed for transfer to HUD in FY 2003 and FY 2004.
[2] This funding is expended as follows: $25 million in Operating Expenses; $23 million in Capital Acquisitions.
[3] This total includes a $33 million change in uncollected customer payments from federal sources.
[4] These totals comprise revolving funds supporting U.S. Coast Guard Academy cadets and the commissary store in Kodiak, Alaska.

Table 2 shows the offices or portions of offices in DHS that are considered to be part of the administrative or managerial capacity of the department. For security reasons, I&A's funding-level allocations are not included but can be provided in an appropriate setting.

The Department of Homeland Security (DHS) classifies its positions in compliance with guidance issued by the Office of Personnel Management (OPM). Position Classification Standards issued by OPM define the various classes of positions in terms of duties, responsibilities, and qualification requirements, and establish official titles. OPM provides the following definitions:

Administrative Work

That which involves the exercise of analytical ability, judgment, discretion, and personal responsibility, and the application of a substantial body of knowledge of principles, concepts, and practices applicable to one or more fields of administration or management. While not all of these positions require specialized education, they do involve the type of skills (analytical, research, writing, judgment) typically gained through a college level education, or through progressively responsible experience. Employees engaged in administrative work are concerned with analyzing, evaluating, modifying, and developing the basic programs, policies, and procedures which facilitate the work of Federal agencies and their programs. They apply knowledge of administrative analysis, theory, and principles in adapting practice to the unique requirements of a particular program. Administrative occupational series typically follow a two-

67123.671

Question#:	16
Topic:	Budget levels
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

grade interval pattern. Administrative functions provide requisite support for the Department's operational functions.

Managerial Work

The authority vested in some positions under the General Schedule which direct the work of an organizational unit, are held accountable for the success of specific line or staff functions, monitor and evaluate the progress of the organization toward meeting goals, and make adjustments in objectives, work plans, schedules, and commitment of resources. As described in 5 U.S.C. section 5104, such positions may serve as head or assistant head of a major organization within a bureau; or direct a specialized program of marked difficulty, responsibility, and national significance. As with administrative functions, managerial work provides requisite support for the Department's mission-driven operations.

DHS Operational Duties

Within DHS, positions with operational responsibilities are those that perform work directly relating to the operations of a DHS Operational Component (as opposed to a DHS Support Component). A DHS Operational Component is a Component with specific centralized program responsibility for directly achieving one or more of the Department's mission activities, and includes the U.S. Citizenship and Immigration Services (USCIS), U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), U.S. Immigration and Customs Enforcement (ICE), U.S. Secret Service (USSS) and Transportation Security Administration (TSA). Such positions would include law enforcement officers, police officers, Secret Service Agents, Transportation Security Officers, etc. Table 3 details the headcount of FTEs of DHS by Components for every fiscal year since the inception of DHS.

TABLE 1: Department of Homeland Security (dollars in millions)

Detailed Table: Total Budget Authority (Excluding Emergency Funding)	FY 2003 Enacted	FY 2004 Enacted	FY 2005 Revised Enacted	FY 2006 Revised Enacted	FY 2007 Revised Enacted	FY 2008 Revised Enacted	FY 2009 Revised Enacted	FY 2010 Revised Enacted	FY 2011 Enacted
	$$$	$$$	$$$	$$$	$$$	$$$	$$$	$$$	$$$
Department Management and Operations									
Office of Financial Operations	2,111.0	394.4	527.3	559.2	600.5	571.3	657.2	807.5	839.3
BTS Under Secretary		8.1	9.6						
CT-Fund 1/		9.9	8.0	2.0					
Analysis and Operations:				252.9	299.7	304.5	327.4	333.0	334.4
Office of the Federal Coordinator for Gulf Coast Rebuilding (OFCGCR):					3.0	2.7	1.9	2.0	
Office of the Inspector General 1/		80.3	82.3	82.2	98.7	108.7	114.5	113.9	113.6
U.S. Customs and Border Protection	5,887.0	5,997.3	6,344.4	7,113.5	7,746.3	9,285.0	11,250.7	11,540.5	11,298.2
U.S. Immigration and Customs Enforcement	3,262.0	3,669.6	3,127.1	3,866.4	4,696.6	5,054.3	5,968.0	5,741.8	5,805.4
Transportation Security Administration	4,648.0	4,578.0	6,068.3	6,167.0	6,329.3	6,809.4	6,992.8	7,656.1	7,687.6
*U.S. Coast Guard	6,196.0	6,994.2	7,558.6	8,268.8	8,554.1	8,631.1	9,624.2	10,789.1	10,203.8
U.S. Secret Service	1,193.0	1,334.1	1,385.8	1,399.9	1,485.6	1,629.5	1,640.4	1,710.3	1,755.3
National Protection & Programs Directorate 2/	-	-	-	-	942.4	896.5	1,188.3	2,429.5	2,331.2
Information Analysis & Infrastructure Protection Directorate 2/3/	185.0	834.3	887.1	-	-	-	-	-	-
U.S. VISIT 2/	380.0	328.1	340.0	336.6	-	-	-	-	-
Office of Health Affairs		-	-	-	9.9	118.4	157.6	136.9	139.5
Federal Emergency Management Agency 4/	-	-	-	4,834.7	8,626.7	9,633.0	10,192.0	10,365.8	10,462.6
Emergency Preparedness and Response Directorate 4/	5,175.0	4,671.8	5,038.3	4,030.8	(6.5)	-	-	-	-
U.S. Citizenship & Immigration Services	1,422.0	1,549.7	1,775.0	1,887.9	2,216.2	2,822.0	2,876.3	2,871.0	2,649.5
Federal Law Enforcement Training Center	170.0	191.6	222.4	279.5	253.3	273.3	333.0	282.8	270.8
Science & Technology	553.0	912.8	1,115.5	1,487.1	968.1	830.3	932.6	1,006.5	827.6
Domestic Nuclear Detection Office	-	-	-	-	481.0	484.8	514.2	383.0	341.7
Office of State and Local Government Coordination	-	4,192.1	3,984.8	-	-	-	-	-	-
Total Budget Authority	31,182.0	35,746.5	38,474.3	40,568.6	43,304.9	47,454.6	52,771.1	56,169.6	55,060.5
(Less Mandatory Fees/Trust Funds)		(5,782.4)	(6,563.1)	(7,063.1)	(7,978.8)	(9,465.8)	(9,528.7)	(10,179.4)	(9,407.6)
Total Gross Discretionary		29,964.1	31,911.2	33,505.5	35,326.2	37,988.9	43,242.4	45,990.2	45,652.9
(Less Discretionary Offsets)		(3,701.7)	(2,993.6)	(2,659.9)	(2,945.4)	(2,923.2)	(3,166.0)	(3,533.6)	(3,442.8)
Net Discretionary Funding		26,262.4	28,917.6	30,845.6	32,380.8	35,065.7	40,076.3	42,456.6	42,210.1

NOTE: Numbers may not add exactly due to rounding.

1/ Funding for the CT Fund and the Office of the Inspector General became separate entities in FY 2004. Before FY 2004, funding and FTE for these two Components were provided under Departmental Management Operations.

2/ Before FY 2007, US-VISIT was a separate Component. Beginning in FY 2007, funding and FTE for US-VISIT was transferred to the National Protection and Programs Directorate (NPPD)

3/ The Information Analysis & Infrastructure Protection Directorate was a separate Component before FY 2007. Beginning in FY 2007, funding and FTE for IAIP was transferred to NPPD

4/ The Emergency Preparedness and Response Directorate was a separate Component before FY 2008. Beginning in FY 2009, all funding and FTE for EP&RD was transferred to the Federal Emergency Management Agency.

QUESTION 16 ATTACHMENT - TABLE 2

Department of Homeland Security
FY 2011 Funding Levels and FTEs

Comp	Programs/Offices	FY 2011 Funding (Whole $s)	FY 2011 FTEs	Comment
DMO	Department of Homeland Security Office of Policy	40,550,176	204	During the 4th quarter of FY11 a below threshold reprogramming removed $582,934 from the Office of Policy after realizing WCF efficiencies to cover one-time priorities in other OSEM offices.
	Department of Homeland Security Office of Policy	15,446,000	1	Reflects 2-year funding transferred from Dept. of State for Afghanistan Civilian Uplift Program.
	Department of Homeland Security Legislative Affairs	6,698,018	31	
	Department of Homeland Security Public Affairs	6,368,016	38	
	Department of Homeland Security Office of the Chief Financial Officer	75,323,140	183	
	Department of Homeland Security Office of General Counsel	23,762,063	131	
	Department of Homeland Security Office of the Chief Procurement Officer	74,597,341	353	
	Department of Homeland Security Office of the Chief Human Capital Officer	46,072,306	130	
	Department of Homeland Security Office of Privacy	8,407,835	34	
	Department of Homeland Security Office of Civil Rights and Civil Liberties	20,367,056	100	
	Department of Homeland Security Office of Chief Information Officer	404,011,157	217	Includes $76.805M in carryover and recoveries.
	Department of Homeland Security Office of Intergovernmental Affairs	2,632,007	27	
FEMA	FEMA Office of Policy and Program Analysis	4,416,983	30	
	FEMA Legislative Affairs	1,817,995	13	
	FEMA Office of External Affairs	12,168,256	88	
	FEMA Office of Chief Financial Officer	26,162,628	249	
	FEMA Office of Chief Counsel	12,160,770	73	
	FEMA Office of Chief Procurement Officer	21,496,280	169	
	FEMA Office of Chief Component Human Capital Officer	19,763,634	178	
	FEMA Office of Privacy	1,125,434	10	
	FEMA Office of Disability Integration and Coordination	150,060	1	
	FEMA Office of Equal Rights	2,638,958	26	
	FEMA Office of Chief Information Officer	52,446,943	434	
	FEMA Office of Administration/Chief Administrative Office	12,465,545	107	
CBP	CBP Office of Policy and Planning	1,359,973	11	
	CBP Office of Congressional Affairs	2,818,797	19	
	CBP Office of Public Affairs	14,579,134	93	
	CBP Office of Finance/Chief Financial Officer	N/A	N/A	Included in the Office of Administration/Chief Administrative Officer line
	CBP Office of Chief Counsel	40,890,739	312	
	CBP Office of Technology Innovation and Acquisition	573,024,654	214	
	CBP Office of Diversity and Civil Rights	7,507,589	72	
	CBP Office of Information and Technology	740,783,077	2300	
	CBP Office of Administration/Chief Administrative Officer	984,139,766	916	
	CBP State, Local, and Tribal Liaison Office	136,134	1	
	CBP Office of Privacy or privacy activities (if such office or activities exist within CBP)	539,285	14	

Department of Homeland Security
FY 2011 Funding Levels and FTEs

Comp	Programs/Offices	FY 2011 Funding (Whole $s)	FY 2011 FTEs	Comment
NPPD	Communications and Public Affairs Office	641,913	5	
	NPPD Budget and Financial Management (NPPD's Budget, Finance, and Acquisitions (BFA))	9,471,702	38	Includes Acquisitions
	NPPD Counselor Legal Advisors Office	N/A	N/A	
	NPPD Office of Privacy	639,000	5	
	NPPD Chief Information Officer	5,595,992	38	
	NPPD acquisition or procurement office or activities (if such office or activities exist within NPPD)	-	-	Acquisitions are included in "Budget and Financial Mgmt"
	NPPD human resource office or Human Capital Officer (if such office or activities exist within NPPD)	5,298,932	34	
	NPPD policy office (if separate office exists within NPPD)	N/A	N/A	Does not exist
	NPPD legislative or congressional affairs	N/A	N/A	
	NPPD office dedicated to state or local outreach or intergovernmental affairs (if such office or activities exist)	N/A	N/A	Does not exist
ICE	ICE Detention Policy and Planning	809,503	5	
	ICE Policy Office (Under Management and Administration)	1,169,765	11	
	ICE Congressional Relations	1,804,262	12	
	ICE Public Affairs Office	6,356,985	48	
	ICE Chief Financial Officer	131,515,586	470	
	ICE Principal Legal Advisor	221,423,000	1396	
	ICE Acquisition Management Officer	22,075,000	202	
	ICE Privacy Officer	590,313	4	
	ICE Chief Information Officer	205,913,000	361	
	ICE State and Local Coordination Office	6,929,797	20	
	ICE Human Capital Officer	50,262,877	184	
	ICE Diversity and Civil Rights*	3,627,830	16	
	ICE Chief Administrative Officer (if this exists within ICE)**	1,220,939	12	
	** ICE Diversity and Civil Rights Office includes CDO and EEO*			
	***ICE CAO does not exist- figures reflect the ICE Office of the Executive Secretariat*			
TSA	TSA Policy Office	N/A	N/A	TSA does not have this office.
	TSA Office of Legislative Affairs	1,107,837	9	
	TSA Office of Strategic Communications and Public Affairs	4,807,953	31	
	TSA Office of Finance/Office of the Chief Financial Officer	24,298,010	147	
	TSA Office of Chief Counsel	34,034,442	197	
	TSA Acquisition Office/Office of Chief Procurement Officer	23,025,453	140	
	TSA Office of Information Technology/Office of Chief Information Officer	406,003	277	
	TSA Office of Chief Technology Officer	1,198,927	173	
	TSA Human Capital Office/Office of the Chief Human Capital Officer	233,409,808	232	
	TSA Office of Administration/Chief Administrative officer	57,581,524	95	
	TSA intergovernmental or state/local/tribal coordination office (if such office/activities exist within TSA)	N/A	N/A	TSA does not have this office.
	TSA Civil Liberties Office (if such office exists within TSA)	N/A	N/A	TSA has an office of Civil Right and Liberties (OCRL) but it is part of a larger office of the Special Counselor and thus, TSA does not have a separate budget for OCRL.
	TSA Office of Privacy (if such office exists within TSA)	N/A	N/A	TSA has an Office of Privacy (OSC/Privacy) but it is a part of a larger office of the Special Counselor and thus, TSA does not have ea separate budget for Privacy.

Department of Homeland Security
FY 2011 Funding Levels and FTEs

Comp	Programs/Offices	FY 2011 Funding (Whole $s)	FY 2011 FTEs	Comment
S&T	S & T Policy and Strategy	-	-	
	S & T Legislative Affairs	-	-	
	S & T Office of Corporate Communications	3,422,873	9	
	S & T Directorate Office of Associate General Counsel	2,325,424	5	
	S & T Director of Finance and Budget	12,887,406	51	
	S & T Director of Admin and Support	11,553,660	25	
	S & T intergovernmental Affairs or state and local coordination office (if such activities and/or office exists within S&T)	1,945,837	7	
	S & T human resources office or Chief Human Capital Office (if such office/activities exist within S & T)	2,305,545	15	
	S & T Chief Procurement Officer/acquisition/procurement activities office (if such office/activities exist within S&T)	10,880,783	-	Funds are for working capital fund expenses in support of S&T procurement operations.
	S & T information office or Chief Information Office (if such office/activities exist within S & T)	11,701,459	15	
FLETC	FLETC Legislative Affairs			
	FLETC Chief Financial Officer	6,774,200	61	
	FLETC Office of Chief Counsel	1,760,700	8	
	FLETC Chief Information Officer	24,903,000	64	
	FLETC Administration	28,924,100	68	
	Policy Office (if such office/activities exist within FLETC)	-	-	
	Public Affairs Office (if such office/activities exist within FLETC-if Washington Operations does this function, please provide information for Washington Operations)	404,000	4	
	FLETC Chief Human Capital Officer human resource office (if such office/activities exist within FLETC)	4,252,400	32	
	FLETC acquisition/procurement office or activities (if such office/activities exist within FLETC)	4,592,800	41	
DNDO	DNDO Product Acquisition and Deployment	1,777,422	9	
	Policy Office (if such office/activities exist within DNDO)	-	-	
	Public or external affairs/communications (if such office/activities exist within DNDO)	94,994	1	DNDO Public or External Affairs/Communications Office is within the Director's Office. 1 FTE assigned to this office
	DNDO Counsel (if such office/activities exist within DNDO)	140,296	1	DNDO Counsel is within the Director's Office.
	Information office/Chief Information Officer (if such office/activities exist within DNDO)	617,411	4	CIO Office is within the Chief Of Staff Office
	Financial management/Chief Financial Officer (if such office/activities exist within DNDO)	903,495	7	Financial Management/CFO Office is within the Director's Office.
USCIS	USCIS Policy and Strategy Office	12,610,000	63	
	USCIS Office of Legislative Affairs	3,496,000	20	
	USCIS Office of Public Engagement	2,141,000	15	
	USCIS Office of Chief Counsel	30,284,000	175	
	USCIS Privacy Office	802,000	8	
	USCIS Management Directorate	606,871,000	1,202	Amount excludes overhead budget.
	USCIS Finance Office/Office of Chief Financial Officer (if this exists within USCIS)	[15,147,000]	[105]	CFO is included in the Management Directorate total is shown here as a non-add entry.
	USCIS Civil Liberties Office (if this exists within USCIS)			
	USCIS Chief information Office/Officer (if this exists within USCIS)	[323,790,000]	[392]	CIO is included in the Management Directorate total is shown here as a non-add entry.
	USCIS Transformation	366,170,000	99	
	USCIS Performance and Quality	6,155,000	35	
	USCIS Enterprise Services Directorate	426,237,000	905	

Department of Homeland Security
FY 2011 Funding Levels and FTEs

Comp	Programs/Offices	FY 2011 Funding (Whole $s)	FY 2011 FTEs	Comment
USSS	Government and Public Affairs Office	12,516,597	79	
	Human Resources and Training	73,832,868	389	
	Office of Policy	3,190,606	13	
	Counselor Principal Legal Advisor	4,494,661	27	
	Administration	40,357,922	192	
	Finance/ Office of the Chief Financial Officer	[5,412,124]	[55]	Included in Administration Total
	Acquisition/procurement/Chief Procurement Officer	[3,180,760]	[29]	Included in Administration Total
USCG	Enterprise Strategic, Mgmt and Doctrine	5,343,288	40	
	Legislative Affairs	-	-	Included in the government and Public Affairs totals
	Government and Public Affairs/Legislative Affairs	7,780,243	67	
	Assistant Commandant for Resources	26,038,710	195	
	Judge Advocate General and Chief Counsel	17,008,696	131	
	Assistant Commandant for Acquisition	57,594,512	420	
	Assistant Commandant for Human Resources	64,078,616	454	
	Civil rights/civil liberties office/activities/Director Civil Rights	3,188,513	23	
	Information technology office (if such exists in United States Coast Guard)	17,344,521	125	

	TABLE 3: Number of DHS Permanent, Full Time Employees by Fiscal Year [1, 2]								
COMPONENT	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009	FY 2010	FY 2011
BTS	59	156	144	99	-	-	-	-	-
CBP	23,811	39,642	41,371	42,665	46,694	51,656	57,435	57,954	59,213
CIS	6	6,389	6,762	7,474	7,971	9,957	10,213	10,082	10,363
DHS HQ	39	192	483	1,097	1,418	1,654	2,199	2,827	3,274
DNDO	3	-	-	38	58	70	93	100	103
FEMA	2,265	2,321	2,293	2,189	2,901	3,401	4,144	4,521	4,794
FLETC	750	838	879	970	1,013	1,009	1,040	1,092	1,084
ICE	34,906	14,394	13,563	14,356	16,475	17,650	19,890	19,585	19,893
NPPD	33	335	535	737	463	563	928	2,443	2,758
OIG	386	449	485	483	515	555	623	624	671
OIP	1	-	-	-	-	-	-	-	-
S&T	69	124	172	214	258	324	367	425	442
TSA[3]	34,514	50,765	50,475	46,965	45,983	49,878	49,188	50,000	51,077
USCG[3, 4]	6,043	6,408	6,825	7,070	7,195	7,369	7,719	7,834	8,324
USM	163	240	384	-	-	-	-	-	-
USSS	4,465	4,622	4,856	5,157	5,246	5,391	5,482	5,656	5,811
Total	107,513	126,875	129,227	129,515	136,191	149,477	159,322	163,144	167,808

Footnotes:

[1] Sources: National Finance Center (NFC) Personnel/Payroll System and the OPM Enterprise Human Resource Integration (EHRI)/Statistical Data Mart (SDM) FedScope system.

[2] Numer of permanent, full time employees for the last pay period of each Fiscal Year. This is not the count of Full Time Equivalents (FTEs).

[3] Number of Permanent, Full time TSA and USCG civilian employees provided by the OPM EHRI SDM FedScope system. In FY 2003 and FY 2004, TSA and USCG were part of the Department of Transportation.

[4] Civilian USCG Permanent, Full Time Employees.

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Question: One of the tasks of the Department is the response to a terrorist attack. The earthquake here in D.C. could be considered a dress rehearsal for a disaster. Cell phones did not work for hours and it was a mess leaving town. There was not a very good evacuation plan in place.

Is it important for the cell phones of private citizens to be operational during an emergency? Is the ability of the average American to communicate in a disaster a capability that the Department thinks is important?

What plan is in place to ease evacuations out of the District of Columbia in an emergency?

How much money has the federal government spent making first responders more interoperable in their communications since 9/11? If any amount of this includes grant funding from the Department of Homeland Security, please provide the levels of grant funding.

How is the Department working on an interagency basis to improve communications in the event of a disaster for private citizens and first responders, including any work with the Federal Communications Commission on broadband access concerns?

What plans and exercises does the Department create or perform that targets the issue of communications capabilities in the event of a disaster for private citizens, first responders, or both?

Response:

Evacuation

During the recent earthquake, an early release of the workforce occurred, not an evacuation. An evacuation is an organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas (National Response Framework, 2008). The District of Columbia has never had a full citywide evacuation, although localized areas of the City are occasionally evacuated for various reasons such as in the case of a fire. As with all the jurisdictions in the National Capital Region, there are evacuation plans in place in the event that the District of Columbia requires evacuation.

67123.679

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

If an evacuation needs to take place, appropriate local officials will notify residents and visitors of potential hazards, incidents, events, and whether it is safest to evacuate or to shelter in place. During an emergency, sheltering in place may be determined to be the appropriate protective action versus an evacuation. Official sources of information can be found at http://72hours.dc.gov, through signing up for emergency text alerts at http://capitalert.gov and through the District's Emergency Voice Alert, or "Reverse 911"system. There are 19 primary evacuation routes out of the District. Traffic signals will be timed to move traffic away from the event/incident area across jurisdictions. Police and traffic control officers will staff critical intersections to expedite vehicle and pedestrian traffic. The District of Columbia, as with all of the jurisdictions in the NCR, regularly communicates with the surrounding jurisdictions and would continue to do so if an evacuation was to occur.

As a Region, the NCR is working on several additional efforts to conduct better messaging and refine their evacuation plans. In April 2010, a DHS- funded project, University of Virginia- published study, *Population Behaviors in Dirty Bomb Attack Scenarios: A Survey of the National Capital Region,* helped emergency planners understand how residents may act if a region-wide disaster were to occur. Currently, Phase Two of the project is ongoing and research is being conducted using focus groups to assess what attitudes employees have about readiness and assess how best to change employee behaviors on readiness and the action they take in a catastrophic event. Also ongoing are updates to Maryland's, Northern Virginia's and the District of Columbia's evacuation plans. The plans are being coordinated on a regional basis and address evacuating citizens out of the NCR and also evacuating citizens towards or through the NCR in various scenarios which may occur in adjunct jurisdictions (such as in Calvert Cliffs or in the Baltimore region).

FEMA also supports field level operational tasks that emergency responders perform within the incident area. Activities include, but are not limited to, conducting initial communications assessments of the various agency needs, distributing fixed and mobile communications capabilities to customers, and providing interoperability through the integration of disparate systems and backup communications capabilities via the National Response Network (NRN).

For example, the purpose of the NCRC Offices' Forward Resolve exercise series is to coordinate and test the interdependencies and coordination of planning efforts for evacuation and shelter in place among federal departments and agencies and their integration with state, and local planning. Last year's exercise brought together the NCR Federal, state, and the local stakeholders to discuss how to coordinate an early dismissal

67123.680

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

during a catastrophic incident or event in the NCR. In March 2012 the Forward Resolve two day exercise will test and evaluate the capabilities of the NCR transportation departments, transportations systems (to include Washington Metropolitan Area Transit Authority and other regional transportation entities), transportation policies, and Regional (S,L,F) evacuation and transportation plans to coordinate, integrate, share information, and manage the release and transportation of citizens and workers from the NCR in the event of shelter in place or an evacuation event. This exercise will also test the mechanisms and methods of coordination and communication, utilized by Federal, state and local agencies, as well as other entities having a presence within the NCR, in response to a catastrophic event. An additional component of this exercise is to identify the degree to which Federal, state and local agencies have the ability to work together in support of the Federal workforce, during an evacuation event.

Private Citizens' Cell Phones

Proper communications saves lives, protect property, and mitigate confusion on the part of individual citizens as well as emergency managers at all levels. The responsibility to ensure that this service is available to the average American, however, falls on private carriers. DHS focuses on the interconnectivity and survivability of the Nation's communications infrastructure to ensure that priority services for National Security and Emergency Preparedness personnel are operational during a disaster.

DHS components, including FEMA and the National Communications System (NCS), collaborate with industry liaisons as part of their Emergency Support Function (ESF)-2, Communications, responsibilities, in providing communications outage and restoration effort situational awareness during emergency and disaster operations.

By April 2012, FEMA's Integrated Public Alert and Warning System (IPAWS) will provide emergency managers who choose to use IPAWS with the capability to send broadcast alerts and warnings to cellular phones via cell carrier networks.

As part of 2011 National Preparedness Month in September, FEMA and the Federal Communications Commission (FCC) released a Stay Connected fact sheet to help prepare the public to communicate more effectively with each other during and immediately following major disasters. The Stay Connected fact sheet provides simple, easy to follow tips to help the public prepare home and mobile devices for use in a major disaster. The fact sheet can be viewed at www.ready.gov/tech or fcc.gov.

Interagency Coordination

67123.681

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

The National Response Framework's Emergency Support Function #15 (ESF#15) Annex identifies the procedures to provide accurate, coordinated, timely, and accessible information to affected audiences, including governments, media, private sector and local populace, including the access and functional needs population during incidents that require a coordinated Federal response. The Department of Homeland Security/Federal Emergency Management Agency is the Primary Agency for implementing ESF #15.

DHS, through FEMA, is working with the FCC, the National Oceanic and Atmospheric Administration, State and local public safety officials and the private sector to integrate additional alert and warning capabilities into IPAWS. IPAWS allows public safety officials to send alerts and warnings via more communications channels to private citizens in affected areas.

The Department, through the National Protection and Program Directorate's (NPPD) Office of Cybersecurity and Communication's Office of Emergency Communications (OEC), is coordinating interagency efforts to improve emergency communications among first responders at all levels. OEC administers the Emergency Communications Preparedness Center (ECPC) to coordinate policy, planning, and administration of emergency communications across 14 Federal Departments and Agencies. The ECPC has achieved early successes through defining a strategic agenda that reflects member priorities and establishes issue-specific focus groups to drive immediate action. ECPC activities include the identification of Federal broadband requirements, development of a consolidated view of emergency communications assets, resolution of associated legal and regulatory barriers, development of coordinated departmental positions on pending broadband regulatory matters and rulemakings, and the establishment of standardized grant guidance and processes.

NPPD/OEC also administers the One DHS Emergency Communications Committee, which aims to improve internal coordination of policy and planning across DHS Components that have an emergency communications mission. This committee, composed of DHS Headquarters and Component senior executives, provides a vital mechanism for maximizing the efficiency and effectiveness of the Department's emergency communications investments and activities. The One DHS Committee reached its most significant milestone in June 2011 with the creation of the unified One DHS Emergency Communications Strategy. The One DHS Emergency Communications Committee is working to provide consolidated departmental input into Federal interagency efforts and to develop strategies for broadband technology migration (e.g., transition from current land mobile radio technology).

67123.682

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

- NPPD/OEC is working closely through the ECPC and the One DHS Emergency Communications Committee on issues related to public safety broadband and the development of a Nationwide Public Safety Broadband Network. The ECPC, including the Federal Communications Commission (FCC), has identified the development of broadband standards and research and development as strategic priorities for the coming year. NPPD/OEC has worked closely with its Federal partners at the Department of Commerce, Department of Justice, and the FCC to help set the broad policy framework for the planned network. NPPD/OEC has also coordinated with its state and local partners—including but not limited to the SAFECOM Executive Committee and Emergency Response Council, the National Council of Statewide Interoperability Coordinators, and the FCC 700 MHz waiver jurisdictions—to ensure the public safety community's requirements are fully represented in network broadband planning and implementation efforts. The President recently signed into law the Middle Class Tax Relief and Job Creation Act of 2012. The bill provides $7 billion to construct a nationwide public safety broadband network, reallocates an additional 10 MHz of radio frequency spectrum to the network, and provides for a strong governance structure, thereby helping to ensure that the public safety broadband network is interoperable, secure and state of the art. Once the bill is enacted, DHS will continue to work with state, local and Tribal public safety agencies, other Executive Branch agencies and the FCC to implement the provisions of the Act.

FEMA created the Disaster Emergency Communications (DEC) Division (DECD) in the Response Directorate to develop policies and operating procedures to facilitate more effective disaster emergency communications operability, survivability, and interoperability. DECD is working closely with the FCC and the NCS to develop policies and procedures to allow the telecommunications industry to improve timely and accurate reporting on infrastructure outages directly affecting the citizen's and first responders ability to communicate effectively. As such, FEMA implemented a tactical disaster emergency communications program to carry out the following:

- Ensure operable and interoperable communications are available in a disaster;
- Provide voice, video, and data communications capabilities for responders and Federal partners; and
- Support emergency communications operational requirements across the entire disaster management lifecycle—preparedness, mitigation, response, and recovery.

67123.683

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

FEMA's DEC works closely with OEC, which serves as the primary federal office for national interoperable emergency communications policy, planning, and analysis. For example, FEMA DEC coordinates closely with OEC, NCS, and the FCC on all 10 of FEMA's Regional Emergency Communications Coordination Working Groups (RECCWGs). The RECCWGS, as established by Congress, are comprised of state, local and federal organizations, and serve as planning and coordinating bodies responsible for providing a forum to assess and address the survivability, sustainability, operability, and interoperability of emergency communications systems at all government levels.

FEMA and the FCC, in coordination with the National Oceanic and Atmospheric Administration administered the first-ever nationwide test of the Emergency Alert System (EAS). The EAS is a national alert and warning system established to enable the President of the United States to address the American public during emergencies. This test was the first time a top-to-bottom review of the entire system had ever been undertaken. The nationwide test successfully generated a comprehensive set of data and identified areas of improvement to help strengthen our national emergency communication system. FEMA and the FCC will incorporate the lessons learned from the test and will continue to work toward a robust, resilient, and fully accessible next generation of emergency alerting system that can provide timely and accurate alerts to the public.

Plans and Exercises

DHS has worked with stakeholders to develop plans and exercises which improve communications capabilities at the Federal, State, local, and tribal level. FEMA has designed, managed and participated in multiple emergency communications exercises. FEMA has recently participated in an interoperable radio exercise with the U.S. Secret Service; a joint exercise with the Transportation Security Administration and the U.S. Army using the Military Affiliate Radio System as a backup in case of widespread devastation, as occurred after Hurricane Katrina. FEMA also designed, managed and participated in the 2011 National Level Exercise focusing on a catastrophic earthquake in the New Madrid Seismic Zone. Before the exercise, states provided information on the types of communications assets they owned. FEMA conducted a scenario-based impact assessment using the information provided and presented the assessment results to the states so they could exercise based on the results. Also, the Regional Emergency Communications Coordination Working Groups (RECCWGS) work with state and local representatives to identify continuity exercises within the region that include communications as a component. Finally, FEMA recently participated in an ESF-2 exercise that simulated operations during the response and recovery phases after an earthquake in Salt Lake City, Utah. Participants included DHS; the Department of

67123.684

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Defense; the General Services Administration (GSA); the U.S. Forest Service; and state, county, and city officials. The exercise provided a better understanding of the roles, capabilities, and authorities of, and coordination with, ESF-2 departments and agencies, and state and local agencies and officials.

In 2007, NPPD/OEC worked with stakeholders from around the country to build Statewide Communication Interoperability Plan (SCIP) criteria and standards under which states would qualify for grant funding through the Homeland Security Grant Program (HSGP) and the Public Safety Interoperable Communications (PSIC) Grant Program. OEC provided technical assistance, outreach, and guidance to states as they developed their SCIPs. In accordance with HSGP and the PSIC Grant Program, all 56 states and territories submitted SCIPs by the December 3, 2007, deadline, and as of April 2008, all 56 States and territories have an approved SCIP. OEC continues to support states and territories in updating and implementing their SCIPs through the annual SCIP Implementation Workshops and technical assistance.

The National Communications System, in concert with FEMA, the FCC, and the National Telecommunications and Information Administration, conducts workshops that focus on the communications capabilities and response efforts related to all aspects of communications, including tactical and infrastructure. The workshops also include exercises designed to identify process and operational issues regarding ESF-2 (communications).

In 2008, NPPD/OEC developed the National Emergency Communications Plan (NECP). Implementation of the NECP has been a key driver behind much of the Department's progress in improving interoperability. The NECP is a strategic document which includes three goals, focusing on response-level communications and providing set standards for emergency response personnel to achieve.

In 2010, NPPD/OEC completed the measurement of Goal 1 of the NECP, which focused on emergency communications capabilities in the Nation's largest cities. To measure NECP Goal 1, OEC worked with 60 urban areas to assess their ability to demonstrate response-level emergency communications during a real-world event in each region. This approach enabled OEC to evaluate their use of emergency communications in real-world settings and in an economically efficient manner.

NPPD/OEC is currently in the process of implementing a Goal 2 measurement, which calls for an assessment of emergency communications performance and capabilities at the county-level. This is a large undertaking, as there are more than 3,000 counties in the United States. NPPD/OEC has coordinated with all 56 states and territories to collect

67123.685

Question#:	17
Topic:	plan
Hearing:	Ten Years After 9/11: Are We Safer?
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Goal 2 results from more than 2,500 counties and county equivalents and is currently working with states to assess the remaining counties. DHS believes the NECP Goals assessment will generate much needed capability data to more strategically direct Federal and state emergency communications resources—including grant funds and technical assistance support—to where they are needed most.

The DHS Science & Technology Directorate is developing a training program that will be ready for a FY13 pilot in communities, which includes public officials, private citizens, private industry, and emergency responders in developing and exercising effective risk communication strategies. The training model will target identification of formal and informal communication networks with emphasis on special populations, framing effective risk warnings, using engagement methods for relationship building prior to events, use of multiple and integrated communication systems (i.e. social media, media outreach, influential leaders, etc.), and evaluating the impact and efficiency of both the messages and communication processes. S&T is working closely with FEMA regions to identify pilot communities once the empirically-based guidelines, trainings, and evaluation tools have been developed.

67123.686

Post-Hearing Questions for the Record
Submitted to the Honorable Robert S. Mueller III
From Senator Joseph I. Lieberman

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

1. Dissemination of Terrorism Threat Information

How would you assess the effectiveness of efforts by DHS and FBI to disseminate threat information to state, local, tribal and private sector entities with respect to the threat stream tied to the tenth anniversary of 9/11? What "lessons learned" do you have from this process with respect to dissemination of terrorism threat information in the future? *(Note: Question also submitted to Secretary Napolitano; may provide joint DHS-FBI answer if appropriate).*

2. FBI Role with Respect to State and Local Fusion Centers

a. How would you describe the role of state and local fusion centers in comparison with the FBI's Joint Terrorism Task Forces and Field Intelligence Groups? How would you describe the ideal relationship among these three types of entities?

b. What are you doing to ensure that FBI offices understand the appropriate role of state and local fusion centers and are effectively interacting and working with them?

c. The Program Manager for the Information Sharing Environment's 2011 annual report (available at http://www.ise.gov) notes that in 2010 all 56 FBI field offices "conducted self assessments on their relationship with fusion centers" which are being used to enhance or refine the FBI's collaboration with fusion centers. What did the FBI learn as a result of these assessments, and how specifically are they being used to enhance or refine the bureau's relationship with fusion centers?

3. FBI Role with Respect to Countering Violent Extremism

The FBI recently set up a countering violent extremism (CVE) office.

a. What is the mission and purpose of the CVE office?

b. Will the office focus on individuals who are in the process of radicalizing but not yet committed a criminal act? If so, how will the CVE office determine which individuals to target with resources? What is the FBI strategy for dealing with such individuals? Will the interagency refer individuals to the CVE office?

c. Where is the office located within the FBI organizational structure?

67123.981

d. How many personnel are assigned to the office?

e. What is the budget for the office?

f. How will the CVE office measure effectiveness?

4. News report of withholding of information to the 9/11 Commission

Recent news reports state that shortly after the attacks of 9/11, the FBI investigated the abrupt disappearance of a Saudi family in Florida two weeks prior to the attack. The news report suggests that the family may have had connections to the 9/11 hijackers. Senator Bob Graham, who co-chaired the congressional Joint Inquiry into the attacks said that the FBI did not provide the information to congressional investigators.

a. Did the FBI provide all information related to this case to the Joint Inquiry and the 9/11 Commission?

b. What was the result of the investigation in Florida? Did it have any relation to the 9/11 attacks? If so, please describe.

c. Did the case have any relation to Adnan Shukrijumah? If so, please describe.

Note:

Responses to these post-hearing questions for the record were not received before the publication of this hearing. Responses received after publication are on file in the committee's offices with the Chief Clerk.

67123.982

Post-Hearing Questions for the Record
Submitted to the Honorable Robert S. Mueller III
From Senator Daniel K. Akaka

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

1. Civil rights and civil liberties advocates have raised concerns about government measures to monitor Muslim American communities. Concerns have been raised about reported FBI home visits, aggressive efforts to recruit government informants, undercover agents in mosques to observe sermons, counter-terrorism trainings that teach that mainstream Muslims sympathize with terrorism, and alleged misuse of the terrorist screening database in targeting Muslim Americans. Aggressive tactics – or even the perception of them – could be counterproductive to preventing violent radicalization and could reinforce terrorist groups' efforts to conflate Islam with violence. These allegations raise concerns about the FBI's approach to interacting with Muslim American communities.

   a. What process does the FBI use to weigh the potential benefits of a particular course of action – such as conducting surveillance in on around a mosque – against the potential risk that such action could hinder future cooperation between the FBI and Muslim American communities?

   b. What is the FBI's approach, and what metrics does the FBI use to assess its success, in establishing and maintaining productive relationships with Muslim American communities?

   c. How does the FBI ensure that its agents understand and respect the constitutional rights of Muslims, in particular the First Amendment protection for freedom of religion and the Fourteenth Amendment guarantee of equal protection under law?

2. One legacy of the September 11, 2001 attacks is that U.S. law enforcement and intelligence agencies now collect, store, an analyze vast quantities of digital data. As a result, for example, there are approximately 400,000 people in the Terrorist Screening Database. How does the FBI ensure that the large quantity of electronic data does not distract authorities from identifying and focusing on real threats?

3. Senators Ron Wyden and Mark Udall have raised concerns that classified interpretations of Section 215 of the USA PATRIOT Act allow domestic surveillance that does not comport with of the public's understanding of what is permitted under the statute.

   a. Please provide a publicly-releasable official interpretation of what types of surveillance activities are authorized by this section of the USA PATRIOT Act, as

67123.983

well as any supplemental classified interpretation the FBI uses to implement the Act.

b. Please explain whether you concur with Senators' Wyden's and Udall's statement that government officials should not describe government authorities in a way that misleads the public, and if so, how you ensure that FBI officials do not describe the authorities under Section 215 in a manner that is inconsistent with the legal interpretation the FBI applies to its actions under the Section.

4. The former Chairmen of the 9/11 Commission released a report on August 31, 2011, listing nine of their recommendations that remain unfinished, including the absence of a functioning Privacy and Civil Liberties Oversight Board. In April, I joined Senators Lieberman and Collins in a letter to the President asking that he nominate a full slate of members so the Board could operate. To date, I have not received a response. What is the status of the Privacy and Civil Liberties Oversight Board being formed?

Note:

Responses to these post-hearing questions for the record were not received before the publication of this hearing. Responses received after publication are on file in the committee's offices with the Chief Clerk.

67123.984

Post-Hearing Questions for the Record
Submitted to the Honorable Robert S. Mueller III
From Senator Mark L. Pryor

"Ten Years After 9/11: Are we Safer?"
September 13, 2011

1. Under the National Strategy for Counterterrorism, one of the core principles guiding our counterterrorism efforts is "building a culture of resilience." The goal of this principle reaches a step beyond preparedness and focuses on promoting an individual and community sense of being able to recover and rebuild from catastrophic events.
   - How do you envision promoting this principle of resilience?
   - How do you measure resilience?

Note:

Responses to these post-hearing questions for the record were not received before the publication of this hearing. Responses received after publication are on file in the committee's offices with the Chief Clerk.

67123.985

Post-Hearing Questions for the Record
Submitted to the Honorable Robert S. Mueller III
From Senator Claire McCaskill

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

1) In your written testimony you stated that the Joint Terrorism Task Forces (JTTFs) are the primary vehicle by which Federal, state, local and tribal law enforcement are integrated with FBI counterterrorism operations.
   a) Can you describe the role of the participating agencies as members of a JTTF? Are all participating agencies given equal access to the intelligence information obtained by a FBI Special Agent assigned to a JTTF?
   b) How are the state, local and tribal law enforcement officers compensated for any overtime incurred or any expenses not covered by their own agency?

2) More than 58,000 Iraqi refugees were granted resettlement in this country after being vetted against existing databases. This included a FBI database which is uploaded with latent fingerprints found on explosive devices. However, there is a backlog of fingerprints that have yet to be uploaded. During your testimony, you explained there is prioritization in terms of the explosive devices that the FBI will look at. Therefore, a print from a lower tiered device may not be in the system resulting in that person being let into the country.
   a) Can you explain the criteria used by the FBI to determine which explosive devices are examined first? From where are the devices originating?
   b) There are other government entities with knowledge of explosive devices. Have you considered asking for their assistance in updating this very important database? If not, how can you ensure the database has the most relevant and timely information?

3) One major priority for this committee and for those protecting our homeland must be to develop and implement measures to detect, prevent and respond to potential cyber threats. During this hearing you testified that the FBI has established the National Cyber Investigative Joint Task Force. I am happy to hear you have established a forward thinking initiative to combat cyber crime. Yet, I would like to know what role the FBI would assume in the event of a cyber attack? If a cyber attack were to occur what measures have been taken to ensure the collaboration of efforts and communication between the FBI and other responding entities, especially DHS?

4) You have previously stated that addressing cyber threats will be among the FBI's highest priorities now and in the years to come. Can you provide more information on what changes or approaches the FBI is taking to demonstrate that addressing cyber threats are a priority for the agency?

Note:

The responses to these post-hearing Questions for the Record were not received before the publication of the hearing. Any responses received after printing are on file in the committee's offices with the Chief Clerk.

The classified responses to Senator McCaskill's questions 2 and 3 are on file at the Office of Senate Security.

67123.993

Post-Hearing Questions for the Record
Submitted to the Honorable Robert S. Mueller III
From Senator Susan M. Collins

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

1. What is being done to ensure that these JTTFs and fusion centers have good relationships and that competition between the two organizations does not prevent much needed information sharing?

2. What is your assessment of how State and local partners are benefiting from the current information sharing environment?

Note:

Responses to these post-hearing questions for the record were not received before the publication of this hearing. Responses received after publication are on file in the committee's offices with the Chief Clerk.

67123.987

Post-Hearing Questions for the Record
Submitted to the Honorable Robert S. Mueller III
From Senator Ron Johnson

"Ten Years After 9/11: Are We Safer?"
September 13, 2011

---

1. In your earlier testimony, you expressed concerns about the number of Federal Bureau of Investigation (FBI) agents dedicated to the task of protecting the nation.

    a. How does the FBI classify its employees in terms of those that are (a) administrative or managerial and (b) those that have operational responsibilities? Please provide the current FTE levels for each of these types of employees within the FBI.

2. You testified that the FBI needed to increase its administration and overhead to integrate and coordinate information and cases.

    a. Please identify which offices or portions of offices in the FBI are considered to be part of the administrative or managerial capacity of the department. Please provide fiscal year 2011 funding levels for these offices or portions of offices and current FTEs.

    b. What plans does the FBI have to tackle the challenges posed by the threat of cyber attacks?

Note:

Responses to these post-hearing questions for the record were not received before the publication of this hearing. Responses received after publication are on file in the committee's offices with the Chief Clerk.

67123.988

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Pryor
Witness: NCTC Director Matt Olsen
Question 1

Question 1: (U) Under the National Strategy for Counterterrorism, one of the core principles guiding our counterterrorism efforts is "building a culture of resilience." The goal of this principle reaches a step beyond preparedness and focuses on promoting an individual and community sense of being able to recover and rebuild from catastrophic events. How do you envision promoting this principle of resilience? How do you measure resilience?

Answer: (U) As you note, the National Strategy for Counterterrorism calls for "a culture of preparedness and resilience that will allow the United States to prevent or—if necessary—respond to and recover successfully from any potential act of terror directed at our nation."

(U) Our federal partners, including DHS and FBI, implement a broad range of programs that promote resilience, including efforts to prevent acts of terrorism, protect critical infrastructure, and ensure rapid and effective responses to catastrophic events. The National Counterterrorism Center focuses on preventing terrorist attacks and countering violent extremism. To this end, NCTC supports the National Security Staff and DHS in the development of the National Prevention Framework as called for in *Presidential Policy Directive (PPD) 8: National Preparedness*. NCTC also is working with the National Security Staff and our federal partners to implement the recently released strategy entitled, *Empowering Local Partners to Prevent Terrorism in the United States*. NCTC initiatives to counter violent extremism—guided by the NSS and carried out in conjunction with interagency partners—have focused on expanding government and community understanding of al-Qa'ida inspired radicalization and violent extremism.

(U) In order to promote resilience to radicalization and mobilization to violent action, we work to educate federal, state, local, and tribal law enforcement as well as community leaders and parents about al Qa'ida and its efforts to recruit Americans. For example, in partnership with DHS and FBI, NCTC developed a "Community Awareness Briefing" to inform members of American communities about the threat of terrorist recruitment domestically and, more importantly, to support efforts at the community level to counter and prevent it. NCTC is working with federal, state, local, and tribal partners to broadly disseminate the briefing to communities around the country.

(U) Our efforts to respond to and recover from terrorist attacks as a cohesive government continue to improve and evolve to meet the ever-changing threat. For example, NCTC, DHS and FBI have collaborated on designing and implementing a Joint Counterterrorism Awareness Workshop Series. This effort is aimed at examining and mitigating gaps and shortfalls in U.S. cities' abilities to respond to Mumbai-style terrorist attacks. The workshops have resulted in tangible improvements in our whole-of-government response, and consequently advanced U.S. cities' preparedness and resilience.

(U) With regard to measurement, the National Strategy for Counterterrorism is the first of its kind to identify resilience as a key element of counterterrorism, and, as a result, we do not have established and reliable quantitative measures for resilience. While measuring our "collective resilience"—the demonstrated ability of individuals and communities to recover from an act of terrorism—is difficult, indications of our level of resilience can be observed by how we as a nation respond to acts of terrorism. For example, our ability to maintain or rapidly restore essential functions; continue economic activities with minimal disruption; and project steadiness and limited psychological impact (including in the levels of political and media attention) in the aftermath of an event would all be potential indicators of our collective resilience.

67123.687

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Pryor
Witness: NCTC Director Matt Olsen
Question 2

Question 2: (U) In your testimony, you mentioned that our counterterrorism efforts include preventing and countering violent extremism, both overseas and at home. One of the tenets that our country is built on is freedom of speech and the freedom to advocate unpopular and even hateful ideas. How do you distinguish between extremists who are venting versus those that might take violent actions?

Answer: (U) We recognize that the rights guaranteed by the First Amendment must be safeguarded, and that freedom of speech is an essential part of our democratic society. We must both safeguard these fundamental Constitutional rights and obtain vital intelligence needed to keep our country safe. To accomplish these dual mandates, we continually draw upon the expertise of our legal counsels and civil liberties and privacy advisors to guide us in distinguishing these often complex issues.

(U) Concurrently, NCTC has been engaged in various efforts to better differentiate between individuals who are solely engaging in protected speech or advocacy from those who are actively planning, preparing or otherwise engaged in ideologically motivated terrorist activities. While extreme views standing alone should never form the basis for labeling an individual a terrorist, we must remain vigilant in identifying and tracking when the threat of violence exists, and taking appropriate action to interdict such threats.

(U) The foundation for NCTC's approach to analyzing violent extremism is to ground its assessments on detailed empirical studies and careful, objective analysis, to distinguish between *beliefs* and *behaviors*, and to focus on the behaviors individuals pursue to prepare for or engage in violent actions to further the goals of foreign terrorist organizations. Our data-driven, behavior-oriented approach has illustrated that there is no single path to violence; rather, a variety of factors can play catalytic or countervailing roles.

67123.688

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Collins
Witness: NCTC Director Matt Olsen
Question 3

Question 3: (U) As a component of the DNI, NCTC was designed to fuse international and domestic intelligence. Several of NCTC's weaknesses were exposed after the failed attack by Christmas Day bomber Umar Farouk Abdulmutallab. In response, NCTC established Pursuit Teams to track specific threats, map and identify terrorist networks, and bridge the gap between international and domestic intelligence operations related to those networks. Can you describe how these new teams differ from other NCTC and IC groups and how they are contributing to NCTC's broader mission?

Answer: (U) The Pursuit Group in NCTC develops tactical leads to pass to operational elements like the FBI, CIA, and DHS, rather than the more strategic analysis that the other analytic groups within NCTC provide to senior policymakers and military officials. It also ensures that all aspects of a terrorism case are explored by focusing on less obvious connections, unknown identities, and seemingly unimportant details.

(U) Pursuit contributes to NCTC's broader analytic and information-sharing missions through its identification of new terrorist leads and its mandate to inform those IC and law enforcement entities that can take action, enhancing the U.S. Government's ability to disrupt threats earlier in their development. Pursuit's unique accesses also allow it to inform its partners when their information would be helpful to the efforts of another agency.

67123.689

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Collins
Witness: NCTC Director Matt Olsen
Question 4

Question 4: (U) Can you describe NCTC's working relationship with CIA's CTC, FBI and DHS and how these relationships affect NCTC's ability to operate and share intelligence with rest of the IC?

Answer: (U) NCTC's relationships with CIA's CTC, FBI, and DHS are strong and increasingly productive. NCTC has several joint initiatives with each agency that enhance the Center's ability to develop new intelligence, strengthen analysis, and ensure that the IC – and the entire USG - has access to the most accurate, timely and useful CT-related information available.

(U) In addition to NCTC's access to "terrorism information" in various "terrorism" datasets, NCTC's current Attorney General-approved US Person Guidelines allow NCTC to access datasets containing domestic terrorism and non-terrorism information in order to identify terrorism information that may be contained within the data, potentially revealing previously unknown relationships to terrorism. To the extent that these datasets are held by agencies such as DHS, CIA and FBI, NCTC and the DNI have worked vigorously to develop bilateral information sharing relationships with these agencies, all subject to stringent civil liberties and privacy controls. The overall approach has enhanced NCTC's ability to analyze and integrate "all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism." NCTC and ODNI are working closely with the Department of Justice and others to update these US Person Guidelines to provide additional operational flexibility while further enhancing the civil liberties and privacy protections.

(U) Today, NCTC analysts can—for the first time—search across key homeland security and intelligence information and get back a single list of relevant results. This information sharing directly benefits all components of the IC. But the information flow is not just one way. Using our unique data holdings and resources, NCTC also provides leads back to the originating agency that supplied the data, as well as leads to FBI for further investigation, when warranted.

(U) Overall, these relationships are integral to NCTC's ability to perform its mission, as well as the missions of the agencies with which NCTC has had the privilege of working:

- (U) FBI provides NCTC with information about many of its CT-related investigations, and supplies NCTC with domestic information and dozens of analysts to help interpret the law enforcement data and facilitate NCTC requests for intelligence sharing with the wider IC. At the tactical level, NCTC's Pursuit Group has established effective working relationships with the FBI to pursue leads and work joint initiatives uncovered through these CT investigations.

- (U) DHS provides NCTC with various datasets related to most of its domestic travel, cargo, and border security, information as well as a number of analysts to help review and interpret this data. Thanks to the successes of this relationship, NCTC has been able

67123.690

to bolster DHS' ability to identify terrorism information contained within its datasets, and has proven critical time and again to NCTC's ability to identify and defend against homeland threats, including those that have arisen on an emergent basis. NCTC and DHS's Civil Rights Civil Liberties staff have placed safeguards to ensure proper handling, retention, and use of U.S. person information.

(U) All of these information sharing relationships are subject to oversight by ODNI's Office of General Counsel, and ODNI's Civil Liberties and Privacy Office, in coordination with their equivalents at the agencies providing the data. Likewise, all data accessed by NCTC is done so in accordance with NCTC's Attorney General Guidelines, supplemented by additional protections for U.S. Persons, as incorporated into individual information sharing agreements with these agencies.

(U) In addition to these bilateral information-sharing relationships, NCTC works closely with CIA, DHS, and the FBI in a number of counterterrorism forums. These include, but are not limited to, the following:

(U) Counterterrorism Resource Council (CTRC): The DNI chairs the council, which is composed of the NCTC Director and key counterterrorism IC partners: DHS Secretary and the Directors of the FBI, CIA, NSA, and DIA. The CTRC served as an important decision and consultative venue for planning the IC's post- 12/25 reforms and continues to pursue key reforms in CT information sharing.

(U) Interagency Intelligence Committee on Terrorism (IICT): The IICT is chaired by the Director of NCTC and is composed of representatives from more than 100 U.S. Government (USG) components. The IICT shares information about CT programs and broad intelligence topics. Topics considered by the IICT include: CT analytic and collection priorities; IC support to USG policies and programs combating terrorism, and procedures for issuing terrorist threat warnings.

(U) Counterterrorism Advisory Group (CTAG): The CTAG is chaired by NIM-CT and is composed of IC representatives from CIA, FBI, NSA, DIA, DHS, NGA, NIC, DOE, Treasury, State, OSC, ODNI, DEA, NCIX, and NCPC. The CTAG covers a broad range of CT issues and activities, including analytic production, collection, strategy, IC performance, and resource issues. The Counterterrorism Strategy Board (CTSB) is the working level forum for coordinating CT strategy implementation and other issues.

(U) The Interagency Threat Assessment and Coordination Group (ITACG), located at NCTC, works with and through DHS and FBI to provide relevant intelligence from traditional intelligence agencies to state, local, tribal, and private sector (SLTP) partners. The ITACG ensures that shared information is both timely, relevant, and transformed into situational awareness products for public safety officials thereby enhancing their capabilities to quickly assess and effectively respond to suspected terrorism and radicalization activities.

Additional SECRET//NOFORN response is in the classified annex held at Senate Security.

67123.691

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Collins
Witness: NCTC Director Matt Olsen
Question 5

Question 5: (U) How have state and local fusion centers added value to the intelligence process at the national level?

Answer: (U) In a constantly evolving terrorist threat environment, state and major urban area fusion centers support the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, and territorial (SLTT), and private sector partners.

(U) NCTC analysts use DHS reporting generated from the fusion centers for both tactical and strategic analysis of threats to the Homeland. The fusion centers, located in states and major urban areas throughout the country, were designed to add value at the state and local levels. Fusion centers provide multidisciplinary expertise and situational awareness to inform decision making at all levels of government. They conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

(U) In coordination with DHS representatives in the field, NCTC domestic representatives frequently interact with fusion centers, sharing NCTC finished intelligence and arranging substantive briefings. In return, fusion centers personnel provide, when appropriate, on-the-ground insight into the details surrounding events that would otherwise be unavailable to the intelligence community writ large, such as information regarding state and local police actions-taken in response to incidents. This type of information has helped clarify for IC elements whether and why or why not local law enforcement assess there to be a terrorism nexus to such events. Additionally, DHS Representatives provide NCTC domestic representatives analytic products from fusion centers for dissemination to NCTC. For example, the NCTC domestic representative has partnered with the DHS representative at the Los Angeles Joint Regional Intelligence Center (LA JRIC) to enable the DHS Representative to directly post LA JRIC products on NCTC's CURRENT-SIPR portal for the benefit of the entire CT community.

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Lieberman
Witness: NCTC Director Matt Olsen
Question 6

Question 6: (U) <u>Lashkar-e Tayyiba Threat to the Homeland.</u> In early September 2011 the FBI arrested Jubair Ahmed, a Pakistani-born US legal permanent resident living in northern Virginia, on charges of providing material support to Lashkar-e Tayyiba (LT). This is the latest example of LT linkages to the United States, the most notable of which was American citizen David Headley's involvement in the 2008 Mumbai attack and a planned attack in Denmark. As you note in your testimony, Director Olsen, LT has not previously conducted attacks against the homeland, but this a concern to the intelligence community. What is your assessment of the threat posed by LT to the homeland today? What factors might lead them to become more focused on directly attacking the homeland and US interests abroad?

Refer to SECRET//NOFORN response in the classified annex held at Senate Security.

67123.692

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Lieberman
Witness: NCTC Director Matt Olsen
Question 7

Question 7: (U) Relationship of Al Qaeda with its affiliates. Has there been an evolution in the relationship of core al-Qaeda to its affiliates since the death of bin Laden? If so, what are the potential implications for the threat posed to the homeland by the affiliates? Do you assess that they are now more or less likely to focus on attacking the United States, as opposed to focusing their efforts in their local areas of operation?

Answer: (U) Al-Qa'ida leaders moved quickly in the aftermath of Usama bin Ladin's death to name his long-time deputy, Ayman al-Zawahiri, as his successor. Since this announcement, the affiliates—al-Qa'ida in Iraq (AQI), al-Qa'ida in the Arabian Peninsula (AQAP), al-Qa'ida in the Lands of the Islamic Maghreb (AQIM), and al-Shabaab—have publicly sworn allegiance and pledged support to Zawahiri, reinforcing the importance of al-Qa'ida core's leadership role in the global movement.

- (U) The death of bin Ladin in May marks a strategic milestone in our fight against al-Qa'ida and is likely to accelerate al-Qa'ida's decline, but does not signal the end of the organization or mute the impact of its narrative. Al-Qa'ida Core remains the ideological leader of the global extremist movement.

- (U) Zawahiri, as recently as August, has publicly reiterated one of al-Qa'ida's core narratives, calling for attacks against the U.S., which bin Ladin also emphasized in many of his messages.

(U) The affiliates have publicly issued threats of retaliation against the U.S. and the West for bin Ladin's death, and at least one, AQI, has already claimed a local attack in the name of UBL. The affiliates are still publicly supporting al-Qa'ida core and its global vision, but continue to focus—as they did prior to UBL's death—on local operations, which may include attacks against local U.S. and Western interests. These groups could, however, take advantage of an opportunity to conduct or support an attack against the Homeland.

- (U) AQIM has threatened U.S. and Western interests in North and West Africa and is likely to continue its operations, which consist largely of kidnap-for-ransom operations and local small arms attacks.

- (U) The Somalia-based training program established by al-Shabaab and al-Qa'ida continues to attract foreign fighters from across the globe including more than two dozen U.S. persons, the majority of whom are ethnic Somalis.

- (U) AQI's August statement claiming 65 separate attacks against Iraqi and Coalition forces in May and June indicates the group remains an active and capable al-Qa'ida affiliate. The arrests in May of two AQI-affiliated Kentucky-based Iraqi refugees underscore the potential threat posed by U.S.-based AQI-associates.

- (U) Al-Qa'ida in the Arabian Peninsula, the group responsible for the 25 December 2009 attempted attack on a U.S.-bound airliner and the October 2010 attempted attack using explosives-laden printer cartridges, suffered a significant loss to its external operations efforts against the U.S. with the recent death of Anwar al-Aulaqi. However, other members of its senior leadership cadre, including its chief bombmaker Ibrahim al-Asiri who is tied to both attempted attacks on the U.S., remain at-large and probably capable of continuing to plan external operations against the U.S.

67123.698

Hearing Date: 13 September 2011
Committee: SHSGAC
Member: Senator Lieberman
Witness: NCTC Director Matt Olsen
Question 8

Question 8: (U) Strategic Operational Planning. A key part of the 2004 intelligence reform legislation creating NCTC directed NCTC to perform "strategic operational planning," referring to interagency counterterrorism planning. The 9/11 Commission had included this function in its recommendation for creation an NCTC. I understand that the NCTC has coordinated the development of an Executive Branch-wide national implementation plan for counterterrorism, created pursuit teams to follow leads, and most recently has been working with the Office of Management and Budget to synthesize a government-wide counterterrorism budget. However, this Committee has heard testimony raising concerns about NCTC's capability to conduct counterterrorism planning – including ambiguity in its mission, shortages of appropriate personnel, and the extent to which NCTC's planning results in action by other agencies.

What is your vision for NCTC's strategic operational planning going forward? For example, what role will NCTC play in translating the Administration's recent counterterrorism strategy and counter-radicalization framework into plans that have objectives, timelines, resources, and metrics?

Answer: (U) Since the creation of NCTC, the role of the Directorate of Strategic Operational Planning has evolved to serve the unique requirements of each administration. As you are aware, there were many different perspectives on what role DSOP should have when the 9/11 Commission first proposed this concept. These different views carried over into the deliberations associated with the development of the Executive Order establishing NCTC in 2004. Ultimately, the vision articulated by your Committee when you and your colleagues wrote the Intelligence Reform and Terrorism Prevention Act in 2004 continues to serve as our vision for the organization.

(U) With respect to the new strategies, DSOP will continue to support the President, when requested, to promote interagency collaboration and integration to ensure seamless implementation and identify gaps in USG efforts to achieve the delineated goals and objectives. DSOP works with OMB to ensure common understanding of resources the USG is applying against the strategies' objectives and to identify areas that require policy maker attention. Under the direction of the National Security Staff, DSOP helps advance these strategies by supporting common understanding of goals and objectives among relevant departments and agencies; identifying USG efforts and activities that contribute to achieving the articulated goals and objectives; and amplifying departments/agencies' roles and responsibilities to ensure wide understanding of equities and complementarities and an integrated whole of government approach. Finally, DSOP can assist the National Security Staff in evaluating progress toward objectives and making recommendations to refine the strategies as necessary by providing impact assessments.

67123.694

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Ten Years After 9/11: A Status Report on Information Sharing
Chairman Joe Lieberman
October 12, 2011

The hearing will come to order. Good morning and welcome to all of our witnesses. Thanks to our witnesses for coming today to help us review the status of information sharing among the law enforcement and intelligence communities at all levels of government in the United States and to determine what, if anything, we still should be doing to achieve yet better information integration, and therefore a higher level of homeland security.

Just yesterday, we witnessed the stunning outcome of brilliant information sharing when the Department of Justice announced it had uncovered a plot to assassinate the Saudi ambassador to the United States, here in the United States. The case apparently began with the Drug Enforcement Administration in Texas and Mexico before it was handed off to the FBI and eventually the Attorney General's office. I presume that members of the intelligence community were involved at various points. The system worked beautifully, the men and women in the field did exactly what they were supposed to do, and as a result we are all safer, including the Saudi ambassador.

This hasn't always been the case, which is why we're holding this hearing. This is the ninth in a yearlong series in which we're assessing progress made on key government functions that the 9/11 Commission recommended we overhaul. Information sharing was a particularly important matter because the Commission concluded that the attacks of 9/11 might have been prevented had our intelligence and law enforcement agencies shared intelligence they had gathered and had in their possession separately to create an overall picture of what was to come on 9/11. Agencies were mired in what the Commission described as a "need to know" culture for sharing information, whereas what the Commission said we should be aspiring to a "need to share" culture.

Immediately after the 9/11 attacks with the focus on this problem, Congress moved to strengthen information sharing among critical federal agencies in the Patriot Act of 2001 and the Homeland Security Act of 2002. Once the 9/11 Commission released its report and recommendations, we worked here on a bipartisan basis to enact the Intelligence Reform and Terrorism Prevention Act of 2004, which tackled the problem in a comprehensive way, particularly by establishing the National Counterterrorism Center to analyze and share information to and from all agencies to better protect our homeland, and requiring the President to appoint a Program Manager in the Office of the Director of National Intelligence to coordinate information sharing across the federal government.

In my opinion, there is little question that our government now operates on a "need to share" basis much more than it did ten years ago. As barriers to information sharing have been taken down over the last decade, the quality and the quantity of information have improved and grown significantly. I think we have also integrated

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.695

important new partners – particularly state and local agencies and the private sector as well - into the information stream.

The results of these efforts are visible in game-changing military and counterterrorism successes that have really protected our security. Shared information, for instance, between the intelligence community and the military led to the strikes that killed Osama bin laden and Anwar al Awlaki. Information sharing among federal, state and local agencies has played a critical role in recent arrests of homegrown terrorists. Some of these are really quite remarkable cases of information sharing, creativity and just plain hard work, particularly including Najibullah Zazi, an Al Qaeda-trained operative who plotted to bomb the New York City subway in 2009, and then the arrest in Seattle in June of two homegrown Islamist extremists who were planning to attack a military recruiting station there.

Unfortunately, we've seen missteps as well. Even when government officials and agencies have information, failure to share enough information combined with human error and technological limitations prevented the detection of Umar Farouk Abdulmutallab before he boarded a plane Christmas Day 2009 and tried to detonate explosives. This Committee's January report of the murders at Fort Hood exposed I think a more serious and ultimately deadly failure of the Departments of Defense and the FBI to share information about the growing radicalization of the alleged killer Major Nidal Hasan, despite what our Committee investigation found were multiple red flags about his behavior.

There are other factors that further complicate efforts to share information. The Wikileaks disclosures exposed the risks of what might be called over sharing, without necessary safeguards. New communications technologies have made it more difficult to ensure that critical information is retained for appropriate use by law enforcement. And of course we have to ensure that information is shared in a way that adequately protects the privacy and civil liberties of our citizens.

Last week President Obama issued an executive order acknowledged that effective information sharing is critical to both national and homeland security, but that in the aftermath of Wikileaks, information must be shared in a secure manner. I think the executive order strikes a sensible balance between protecting information from unauthorized disclosure and coordinating information sharing across all levels of government. Now we need to make sure the executive order is implemented fully and expeditiously.

So bottom line as we meet today on this subject is we have come a long way since the failures of information sharing that helped to enable the attacks of 9/11, but we must continue to build on that progress if we are to maintain our security, and that's what we hope this hearing will help our Committee do and why we're so grateful to have a truly excellent panel of witnesses before us.

Senator Collins?

67123.696

Statement of Ranking Member
Susan M. Collins

"Ten Years After 9/11: A Status Report on Information Sharing."

October 12, 2011

The results of information sharing and collaboration within the Intelligence Community were evident in the operations that located, tracked, and killed Osama bin Laden and Anwar al Awlaki and just yesterday, in the disruption of a plot by elements of Iran's government to kill the Saudi ambassador to the U.S. on American soil. This appears to be another victory for the cooperation across departmental boundaries.

When the Chairman and I were working on the Intelligence Reform Law in 2004, we understood it would be challenging to change the culture in the intelligence and law enforcement communities from "need to know" to "need to share."

It is gratifying that many intelligence and law enforcement professionals have embraced this change. In a recent op-ed, Director of National Intelligence James Clapper observed that the Intelligence Community now starts "from the imperative of 'responsibility to share,' in order to collaborate with and better support" its intelligence consumers, "from the White House to the foxhole."

United States Attorney Patrick Fitzgerald more colorfully told an audience last month that intelligence and law enforcement operators now ask themselves: "[I]f it's found out that I have information that I didn't share with someone, how am I going to justify to myself that I sat on it?" He could have added: How will the failure to share be justified to Congressional overseers or, far worse, to the victims of a successful attack?

I believe the influx of new analysts who joined the Intelligence Community after 9/11 has had a real impact on information sharing. This new generation of intelligence officers is much more comfortable sharing information; social media and collaborative information technology have been a daily part of their lives. It just makes since that they would incorporate those same tools into their work.

Notwithstanding recent successes, however, the GAO continues to rank terrorism-related information sharing as a high-risk area. And, as we saw in the Fort Hood attacks and the attempted airplane bombing on Christmas Day 2009, when information is not shared, our nation's security is placed at risk.

The Bowling Green, Kentucky, case is another recent example of information apparently not being shared, and it remains very troubling to many of us.

67123.697

It is unsettling that a suspected bomb maker, whose fingerprints we had had for years, was able to enter our country on humanitarian grounds.

I have raised this issue repeatedly with the Secretary of Homeland Security and the FBI Director. Both have told this committee the 58,000 individuals who have been settled in the U.S. have been vetted against the existing databases. But it is clear that those databases are still incomplete. Forensic information being collected from IEDs in war zones should be shared and used to screen those seeking to enter our country.

In some respects, these cases may demonstrate an evolution of information sharing: As more and more information is being shared, it is increasingly important for agencies to think creatively about how best to prioritize, analyze, and act upon that information. As this Committee concluded in our investigation of the Fort Hood shootings, the Defense Department and the FBI collectively had sufficient information to have detected Major Hasan's radicalization to violent Islamist extremism, but they failed to act effectively on the many red flags signaling that he had become a potential threat.

As Wikileaks breach demonstrates, we also need to secure data from internal threats. We must be vigilant, however, to ensure that such security measures do not recreate old stove-pipes. Technology and innovation should ultimately help protect data from unauthorized disclosure, while facilitating appropriate sharing of vital information.

Just last week, the President signed a new Executive Order on "Responsible Information Sharing" prompted, in part, by the Wikileaks situation. This hearing should help us assess the President's new order.

The President's new Executive Order will create a "Classified Information Sharing and Safeguarding Office" within the Information Sharing Environment we established in the 2004 law. Unfortunately, according to GAO, this framework is still not as strong as it could be.

As we explore the issue of information sharing, we must also ensure that our homeland security partners, like local law enforcement and fusion centers, are receiving and sharing information that is useful and adds value. Among other things, the Intelligence Community must clearly identify what sorts of data are needed, so state and local partners can be on the lookout for the most useful bits of information.

The public should be able to share its information too. This is why Senator Lieberman and I introduced our "See Something, Say Something" bill, so the public can more easily share – and law enforcement professionals can act on – their tips.

Finally- I would be remiss if I did not express my concern over this administrations inexplicable failure to fully appoint and staff the privacy oversight board that we created as part of our 2004 act. I am truly baffled by the administrations slowness in this regard because it is an important check as we seek to expand information sharing. From the most sophisticated intelligence collection methods to the police officer on the street to the observant sidewalk vendor, information sharing is key to keeping our fellow citizens safe.

67123.698

October 12, 2011

Statement for the Senate Committee on Homeland Security and Governmental Affairs

John McLaughlin

Distinguished Practitioner in Residence
Paul H. Nitze School of Advanced International Studies
Johns Hopkins University
1619 Massachusetts Avenue, NW
Washington, DC 20036

Thanks for asking me to join you today as you delve into this most important subject.

The requirement to share information and the challenges associated with this have been around since time immemorial -- and most pointedly perhaps in the profession of intelligence.

Ancient writers such as the Chinese strategist Sun Tzu capture the essential dilemma in stressing both the need to know everything about your adversary and the need to protect what you know from compromise. But Sun Tzu did not have to struggle, as we do, with the global information net, highly sophisticated encryption, complex legal norms designed to protect privacy, and the massive volume generated by things like a ceaselessly expanding internet, SIGINT agencies that, at least in theory, can collect the equivalent of the Library of Congress in three hours, and electronic media that, when found on the battlefield, may contain the equivalent of a small public

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01081 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.699

library. If I can use a metaphor I hate, Sun Tsu had many fewer dots to find, much less connect.

In the end, information sharing is not sharing for sharing's sake. It is sharing to increase the chance of discovering things that may be in the data. So our problem is less a matter of collecting information than it is a matter of discovering what's in it – essentially finding the "bad guys" or the worrisome trends.

If there is a key point here it is probably this: Despite the always critical importance of individual intuition, drive, and performance, we are long past the point when we could rely on single individuals or a single human brain alone to absorb, remember and correlate everything required to ferret out people with ill-intent or developments that portend trouble.

In today's world, success in that requires an unprecedented level of cooperation among people with varied expertise, supported by information systems that make that easier, and legal systems and procedures that take all of this complexity into account.

In formulating my thoughts on this, I am drawing on two things: my own experience in counterterrorism in the first four years after 9/11 and, more recently, the study that I and three other panel members completed for the DNI in 2010, focused on the 2009 attempted Christmas bombing and the Ft. Hood shootings.

So I'd like to cover two things in the next few minutes: First, some positive and negative trends affecting information sharing; second, some suggested ways to move forward.

So, let me begin with three positive trends:

First, I think the desire and willingness to share information have increased dramatically since 9/11. It was never as bad before 9/11 as critics imagined, but we are clearly in a different place today. There are still parochial pockets of people who don't understand the benefits, but the momentum is clearly in the other direction.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01082 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.700

Let me be clear, I don't think of sharing as a kind of "nice to have" – that is, we don't need to share just out decency and fraternity. The need arises because different perspectives, different data streams, and varied expertise are necessary to figure things out.

Second, capabilities for sharing have improved, but mostly within agencies. Every major agency has one or several showcase programs that make data access and analysis markedly easier and more effective than even five years ago. Some of these programs are world class impressive. A problem is that most of these programs are within individual agencies and, especially for raw reporting databases, do not operate very effectively across agency lines. A noteworthy exception is the sharing that takes place within the confines of the National Counterterrorism Center (NCTC), which brings together in one place databases from many different agencies.

Third, there is an improved policy foundation for access to and sharing of data. I refer mainly to Intelligence Community Directive (ICD) 501 that contains the essential tools – admittedly hard to implement – that should allow those seeking answers to discover what relevant data exists, request access to it, and have that request professionally and fairly adjudicated.

Those in the Director of National Intelligence Office charged with implementing ICD 501 have a detailed plan that has now moved successfully through the first two phases and has at least two phases to go. Progress is slow but steady.

But there are at least three countervailing or negative trends:

First, the volume of data keeps going up – with no end in sight – ensuring in the process that those who would do us harm can often go unnoticed without even trying that hard. This flows largely from the fact that we are in the midst of a technological revolution unrivaled by anything in history other than perhaps the invention of the wheel.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01083 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.701

In 1952, the year the National Security Agency was created, there were about 5000 computers in the world. Today we have an internet population in the billions surfing through sites that number in the hundreds of billions. Computing power in the world doubles at least every 18 months, largely due to the ongoing miniaturization of electronic circuitry; in 1982, the average microchip had 29 thousand transistors – today it has about a billion. All of this gives the adversary more tools and more places to hide; of course it does the same for us.

These days, it is not uncommon for an intelligence analyst to see his or her daily "take" of messages go from hundreds to thousands overnight. So information sharing is not just about ensuring that information moves across agency or organizational boundaries; it is also about ensuring that individuals receiving data can actually see, comprehend, and assess what is arriving in their "in-boxes".

Second, the breakdown in security discipline in our own government works against sharing of information. Leaks, both unauthorized and authorized, strengthen the impulse to tighten up -- and they reinforce the arguments made by those who stress the risks in sharing and pose obstacles to doing so.

And third, despite the progress represented by ICD 501 -- broader policy, procedure, and law have been slow to keep pace with the challenge. I'll elaborate on this in a minute.

Given this complex picture, what is the way forward? I regret to say that there is no formula for perfection, given that we are dealing with truly revolutionary trends in the production of information.

But that does not mean that we cannot dramatically improve the odds on our side.

To do that, I would emphasize the need for progress on two areas:

First, we need finally to break through the barriers that have for years kept us from bringing the most advanced information technology to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01084 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.702

bear on the problem. As I said earlier, we have reached the point where we simply cannot count on the human brain alone to do all the work; in fact, I would go so far as to say it is unfair to intelligence, law enforcement, military officers and our diplomats to do so.

The volume is too daunting, the clues too fragmentary, deception techniques too numerous, and the workforce too stretched. Of course, information technology itself cannot solve the problem – but it can prompt humans to look in all the right places, consider pieces of data that might otherwise be missed, and expose relationships that are buried in all the "noise" that this avalanche of data represents.

What stands in the way?

I have not recently had the opportunity to gauge progress, but the last time I checked there were three mega issues standing above all the particular ones down in the weeds.

First, there is in the national security community limited visibility into data that is distributed across multiple separate systems housed in individual agencies;

Second, existing search capabilities do not allow full exploitation of existing data;

And third, there is not a common and widely-shared vision among national security specialists of the end state they want to achieve on information technology and information sharing. Without such a commonly shared end state, it is hard to make the tough decisions needed to get there.

Going deeper into the weeds on this, there are a number of things that deserve attention in the near term, medium term, and longer term.

To give just one example for each:

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01085 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.703

In the near term, it important to have more on-line instruction for national security specialists on what data bases exist and what you can expect to find in them.

In the medium term, we should work to improve search capabilities and training in how to use them.

In the longer term and once basic capabilities are improved, we need to introduce more software capable of exposing underlying relationships in large bodies of data – to borrow a phrase from the Markle Foundation's study of this, we need to get to the point where "data talks to data".

If there is one thing that stands in the way of this kind of progress, it is the age old tension between the need to share and the need to protect the information we acquire, especially that gained through intelligence means.

Both sides have valid arguments. Failure to share means that we will not draw on the expertise of everyone able to contribute to solving problems and defending American interests. Failure to protect means that we risk exposing sources, the identity and plans of our officers, and sensitive intelligence methods.

This is merely a technological age manifestation of an ancient intelligence dilemma: the ever present clash between the need, on the one hand, for prudent risk-taking and, on the other hand, the requirements of smart counterintelligence.

Faced with a dilemma like this – really a sort of Gordian Knot in the intelligence profession – leads me ask what management theorists call the "paradigm shift question": What is it that, if we could do it, would revolutionize what we do?

The intelligence officers who figured out how to take photos from space in 1960 were probably answering that question, even though they probably had never heard a buzzword like "paradigm shift".

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01086 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.704

So what is it that would lead to a breakthrough on information sharing? The closest I can come up with is something easier to say than to do: a common standard for access to data – essentially the virtual equivalent of an intelligence community badge, the innovation that now lets intelligence officers move physically among different agencies.

This would mean for example that an NSA officer would be able to log on through the same portal, or home page if you will, as everyone else in the community to access, let's say, CIA or FBI data, and that CIA and FBI would have confidence that they know who this person is and what they are authorized to access. It would go a long way to giving assurance to those who rightly worry about the counterintelligence threat.

This would need to be backed up by common standards and processes in every agency for data services such as the auditing, processing, storage and retrieval of information.

I don't minimize the difficulty of doing this: it would take decisive leadership, a shared vision, substantial personnel and financial resources, and buy-in from congressional oversight. But unless we do something like this, we'll just keep having the same old argument until the next bad guy gets through the wire.

The second broad problem likely to complicate our efforts, especially the need to identify people inspiring, aiding, or intending to carry out terrorism, is that so many of them are turning out to be American citizens. The names of al-Aulaqi, Najibullah Zazi, David Headley, Faisal Shazad, and – in the last 24 hours – Manssor Arbabsiar are familiar ones in this room. Others are undoubtedly lurking in the mountains of data we are scooping up daily.

This is a problem with at least three dimensions, and I believe efforts are underway to deal with all of them:

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01087 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.705

First, I suspect there is still an inconsistent understanding of the laws and regulations that govern the acquisition and sharing of data that touches American citizens;

Second, there is an understandable concern not to violate laws protecting our citizens' privacy. This can inspire a subtle kind of "risk aversion" in dealing with such data.

Third, terrorists in my personal view have figured all of this out. Faisal Shazad, the unsuccessful Times Square bomber, got his US citizenship a year or so before carrying out his act. Such people know that this complicates our task in detecting them.

Finally, looking to the future there is no chance that this is going to get easier. With each incident – the Christmas bomber, the Times Square terrorist, the package bomb plot, the attempt to implant explosives surgically in terrorist operatives – our adversaries seem to be devising strategies that are harder to detect, while systematically exploiting our vulnerabilities.

Information sharing is a huge subject, so I've chosen to focus on what I judge to be the major problems frustrating the unquestioned dedication and hard work of intelligence officers in this most difficult and complex of times. I am very aware, that whatever shortcomings there are on counterterrorism stand out because they are so at odds with the broad pattern of success our intelligence, law enforcement, and military officers have delivered since 9/11.

As always, intelligence successes are rarely apparent, not only because we cannot talk about them but because they are usually woven invisibly into the fabric of policy successes.

Thank you for the opportunity to testify, and I would be glad to take your questions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01088 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.706

Written Testimony of Thomas E. McNamara
Committee on Homeland Security and Governmental Affairs
Wednesday, October 12, 2011
Dirksen Senate Office Building – SD 342

I am Thomas McNamara and from early 2006 until mid 2009 I served as the Presidentially-appointed Program Manager (PM) for the Information Sharing Environment (ISE). This position is administratively located in the Office of the Director of National Intelligence (ODNI), but its statutory authorities and mission extend beyond the Intelligence Community to the entire federal government, and include responsibilities for information sharing with state, local, tribal, and foreign governments, and the private sector – i.e. the ISE Stakeholders. It is again a pleasure to testify before this committee. During my 3 1/2 years as PM, I had the pleasure to work closely with its members and staff, from whom I received encouragement, constructive criticism, and strong bipartisan support. For that, I thank the committee and especially the Chair and the Ranking Member.

Congress established the PM-ISE specifically to address deficiencies identified by both the 9-11 and WMD commissions. It mandated the creation of an ISE to ensure that those responsible for protecting our nation from future terrorist attacks have access to the information they need to be effective. Hence, I directed very intense, broad efforts to design, create, and develop sharing among ISE stakeholders.

I will not redundantly describe the ISE or the PM's Office to this committee. For others reading this statement, let me note for the record that the ISE has been built with the objective of sharing the right information with the right individuals at the right time throughout the government structures of the nation. This can only happen through balanced ISE access and control methodologies and technologies, which are well known, and already widely used in the private sector.

Two years ago in my final appearance before this committee as the Program Manager, I stated that we had built a strong foundation for the ISE, but that a fully functional, mature ISE was still a desideratum. I am delighted to observe two years later that the ISE has gone well beyond that point.

A truly mature and functioning ISE can only exist when we have fully rationalized, standardized, and harmonized rules, procedures, and operating systems to manage the ISE. To get from the start point to that fully mature system is -- we now know -- a long, complex, and difficult process. Today, ten year after 9/11 and five after I sent the required Program Manager's Implementation Plan to the Congress, we are, well beyond the foundation, but we are not near the finish.

What I find most encouraging in the last two years is that the pace and breadth of change are stronger and more widespread among all stakeholders. Concepts and programs that were hard-fought struggles in those first years are accepted as conventional wisdom, now. CUI, to cite one example, was met with widespread skepticism and open opposition, when in 2006 we set the goals and began building the CUI structure. Today, CUI is a fully accepted tool of information management in the federal government, and is championed enthusiastically by state and local governments. CUI problems lie in refining the structure, getting resources to transition to CUI from the SBU markings, and solving new problems that occur because CUI is up and running. I know of no agency, now, that opposes CUI, or believes the old way was better. From my perspective, that is huge progress. Even these new problems demonstrate progress.

67123.707

At the macro level, my observation is that the ISE is alive, well, and growing stronger. There are many cases of agency resistance to change in particular circumstances, and there are significant systemic problems, only some related to inadequate resources. There is not, however, the pervasive resistance to change that we faced five years ago. We had to spend much time getting "buy-in" from stakeholders who were skeptical or hostile about spending resources on the ISE. This is normal in large bureaucratic organizations, which, like a supertanker, change direction slowly at first. When the ship finally swings, however, it keeps swinging and the job of the captain is to direct the energy and the attention to stay on the desired course. At the macro level, I believe current plans and strategy are sound for reaching our goal of a mature ISE. I believe we are on course.

At the micro level, however, we have not finished creating all the standardized and harmonized rules, procedures, and operating systems that we need. The incomplete standardization and harmonization are the central problems of today. To get all the energy focused on achieving the desired outcome, is not easy. Different agencies and levels of government have different priorities, different resource constraints, and different levels of capability. Also, growing the ISE causes it to "bump" into other programs and priorities, which are out of step with the ISE and/or have conflicting priorities. In short, a growing ISE interferes with other big "rice bowls."

Managing and coordinating, when such differences exist, has it own difficulties. I know the committee has examined Wikileaks, and I do not intend to focus on it here. The Wikileaks disaster, however, makes this point emphatically. Two agencies – neither opposed to sharing information, and both trying to implement ISE goals and objectives -- had non-standard, non-harmonized ways of managing the same information. Also, policies and rules for information sharing lost out to a higher priority program, viz. giving the "war fighter" whatever data the war fighter might conceivably need.

Had there been standardized and harmonized rules, both agencies would have known how information is properly managed, would have managed it that way, and been confident that the other was managing it properly. Viewed in this way, Wikileaks is evidence of growing pains in the ISE. It was a huge mistake, but one that a developed and mature ISE can prevent. Indeed, the President's Eexcutive Oorder (EO) of last Friday mandates actions to avoid this and other growing pains. This EO is a big step in the right direction.

I take it, also, as a proof of the changed attitudes about information sharing, that there was no hue and cry to end information sharing or to close the Program Manager's office following Wikileaks. I dare say, had Wikileaks occurred in 5 years ago, the ISE would have been stopped in it tracks. As this committee knows, there were efforts to shut down PM-ISE while I was PM and, thanks to this committee, they were unsuccessful.

What has happened, I believe, is a transformation of attitudes. We have all seen the absolute necessity of managing information in the new information age, using policies and procedures that respond to the needs of the new age. We may pine for the "good old days," but we can never go back to them. There is simply too much information and too many organizations and individuals requiring information to think government can function properly without an ISE. The rest of our society has moved with alacrity into this new information-sharing world. Government must follow.

67123.708

Let me list what I consider the major accomplishments, thus far, in building the ISE from its very inauspicious beginnings. All but one item on my list was non-existent, even in concept, in 2001. Only a few things on this list were nascent in 2006, either struggling to gain acceptance, or to prove themselves. Everything on this list is a functioning program today, providing improved security to the nation at every level of government.

- **National Network of Fusion Centers:** The concept of fusion centers predates 9/11, but the nationwide drive and investments in them by federal, state and local governments grew exponentially after that tragedy. Today, this "central nervous system" of the ISE is a true national network whose full potential is being realized. It is one of many examples in the ISE of the federal system working well. The task before us is to ensure fusion centers are not focused only on terrorism, but have a true mandate for all crimes, all hazards. We also need to foster better cooperation, collocation, and some forms of integration of fusion centers with other similar centers (e.g. JTTFs and HIDTAs) to create a truly national asset for all law enforcement and all first responders. There is no good reason why this cannot and should not be done.

- **Controlled Unclassified Information (CUI):** I have already spoken of this. CUI is a huge task because the amount of CUI is orders of magnitude larger and more complex than classified information, and is widespread in every agency of federal, state, and local government.

- **Suspicious Activity Reporting (SAR):** When the Program Manager took on the task of making a useful tool out of a nationwide blizzard of local police reports (SARs); others had already failed in the effort. The difference was the PM had people with federal and local police experience who thought outside the box. Within a year we had an implementation plan, a pilot program, and most importantly, the support and participation of major local and state police departments. It was these latter – another example of federalism -- that taught the PM/ISE how to manage SAR. Today, SARs are an extremely valuable tool at all levels of law enforcement.

- **National Information Exchange Model (NIEM):** The unsung hero of the ISE is the NIEM, which provides the technical foundation for ISE information exchanges around the country. From its modest beginnings in the Department of Justice in 2005, it has expanded with the strong support from PM/ISE through all levels of government, the private sector, and in the future, internationally among our allies and partners. It is the engine on which the ISE exchanges information. It too functions for non-terrorism information.

- **Privacy Rights and Civil Liberties (PR/CL)**: As NIEM is the technical foundation, so PR/CL Guidelines provide a policy foundation for a successful ISE. It has always been, and remains, job one of the Program Manager to formulate, propagate, and ensure PR/CL rules are observed by all ISE users. The past five years have produced a viable, replicable methodology to monitor and oversee the PR/CL policies, so essential for public acceptance and support of the ISE. Of all the things I took pride in as PM, the PR/CL program was at the top of the list. Without it, support for the ISE will wither and die. It has been so well constructed that it, also, is a valuable template for non-terrorism information.

67123.709

There is also a list of the highest priorities remaining to move the ISE to the next higher, more effective, more secure level. Here are, in my opinion, some of the major problems, which need attention:

- **Monitoring and Auditing:** The ISE was never envisaged to give access to information until control mechanisms are adequate to ensure that only the right information flows to the right people at the right time. Such controls are accomplished, as mentioned above, through standardized rules, procedures, and operations. This must include programs for adequate monitoring and immutable auditing -- the information assurance function. In these areas the ISE has not reached the levels necessary for a fully functioning environment. The priorities, the attention, and the resources for these functions remain inadequate. In a huge bureaucracy, including federal, state, and local government, the challenges are formidable. But, the ISE will ultimately fail unless these critical functions are developed and implemented. I was pleased to see these areas included in last Friday's EO to protect against the "insider threat." That is another step in the right direction.

- **Discovery and Authorized Use:** Closely related to the above are two functions that are the most difficult and complex to implement, and yet are certainly indicative of a fully developed, mature ISE. In a sense "discovery" or "discoverability" is no more than a better variant of the "tear-line" approach in the old information system. Individuals can "discover" if information exists on a subject, even when they are not authorized to see it. Authorized use (also called ICA - Identity authentication/Credentialing/Access) allows a person to be recognized and authorized to use the ISE for the purpose and role attached to that individual. The beginnings of this function can be seen in several communities (e.g. law enforcement, intelligence, homeland security), but not for all users, and not across systems and agencies at all levels of government. Nevertheless, the startup of these two essential functions is progress, and I hope that the progress will continue and result in a true cross-government system of "authorized use" or ICA.

- **Interoperability across Networks:** With the security of the ISE assured through effective monitoring and auditing, and the identity of all users pinpointed through an effective authorized use function, greater interoperability across networks at given security levels is possible. This function is less complicated that those I mentioned above, but its use in the ISE will be possible only to the extent that the other functions are put in place.

- **Expanding the Mandate:** Finally, I take this opportunity to point out, again, to this committee and the Congress an anomaly in building the ISE. The legislative mandate for the PM is to build the ISE for "terrorism-related" information only. The above functions demonstrate that they transcend the "terrorism-related" mandate. Although the Program Manager only has authority for managing terrorism information, no agency partitions off terrorism information from its overall information management systems for all classified or CUI information. This is why, as Program Manager, I insisted that the ISE functions be designed to apply in an information management system for all classified and CUI information. That reflects my conviction that it is impossible, and undesirable, to create a "Terrorism-only" ISE. The mission is to create a broad-based ISE. The mandate and authorities should reflect that mission. Last Friday's EO took a

67123.710

small step in that direction. It is, however, more than time for that expanded mandate to be created.

Let me close by summing up what I think can be the future of the ISE. Two years ago in saying we had built the foundation, I used a Churchillian turn of phrase: that we were not at the beginning of the end, but at the end of the beginning. When I look back now, I can see that we are well beyond the end of the beginning. But, when I turn around and look forward, I can see that we still have a long way to go to get to the beginning of the end. We are, however, moving faster, more efficiently, in the right direction.

I estimate that today we are at the half-way point. Since we are moving faster, I expect that we need less than five more years to reach that goal we set five years ago – a fully developed, fully mature ISE. With the support of the Congress and the White House, and continued focus on raising the ISE to higher levels, we can get the job done.

We must get the job done. The 9/11 and WMD commissions were correct, faulty information sharing was a major cause of that tragedy. Long before 9/11 and since, almost every failure to spot and stop attacks on the homeland shows that defects in information sharing were part of the problem. Every success, then and now, has shown that information sharing can make our job easier and more successful. We owe it to the nation to speed the process, stay the course, and achieve the goal.

Thank you, and I will be pleased to try to answer any questions you may have.

67123.711

Government of the District of Columbia

Metropolitan Police Department

Testimony of
Cathy L. Lanier
Chief of Police

Ten Years After 9/11: A Status Report on Information Sharing

United States Senate
Committee on Homeland Security and Governmental Affairs
Honorable Joseph I. Lieberman, Chair
Honorable Susan M. Collins, Ranking Member

October 12, 2011

U.S. Senate
342 Dirksen Senate Office Building
Washington, DC

Chairman Lieberman, Ranking Member Collins, members of the Committee, staff and guests – thank you for the opportunity to present this statement on the status of information sharing among federal and local partners. I am the Chief of Police of the Metropolitan Police Department of the District of Columbia, the primary police force in the nation's capital. As the Chief of a major city police department, I am very pleased to be able to brief you on the significant progress made in federal—local information sharing, and how that has improved our ability to safeguard the public.

In my testimony, I will elaborate on why it is even more important now, ten years later, to recognize the vital role of local law enforcement in our homeland security efforts. With threats to the nation constantly evolving, local law enforcement officers who are on the street every day are uniquely positioned to detect and prevent terrorist incidents. There are more than 700,000 law enforcement members across the nation that know and are connected to the communities they serve, placing them in the best position to detect and investigate criminal activity that might be connected to terrorism or violent extremism. Clearly, information sharing with local police is essential to countering the threats we face going forward.

The success of local law enforcement in fulfilling our role hinges on the cooperation and support of our federal partners. Ten years after the September 11th attack on the United States, the partnership between federal and local authorities is robust and continues to improve. The ten year anniversary of 9/11 presented an excellent case study to illustrate how the infrastructure and relationships we have built operates in critical situations.

Important groundwork for the anniversary preparations was established in 2010. With a significant increase in American citizens or residents aligned with violent Islamic extremists arrested or convicted in 2009, the Department of Homeland Security (DHS) launched a broad working group on Countering Violent Extremism (CVE). From the outset, this working group included local law enforcement. Following that effort, DHS and the Federal Bureau of Investigation (FBI) committed to a partnership with MPD to engage and educate our partners in the private sector and the community. Beginning in 2010, we jointly briefed thousands of government and private sector partners around the National Capital Region on recognizing and reporting suspicious activity, as

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01095 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.713

well as responding to potential terrorist threats. Those briefings certainly paid off, as you will see, when we entered the high threat period of the 9/11 10-year anniversary.

Fast forwarding to last month, early on the morning of September 8, 2011, I received virtually simultaneous calls from my own official in the Joint Terrorism Task Force (JTTF) and my counterpart at the Department of Homeland Security urging me to attend a classified briefing on an emerging threat to Washington, DC, and New York. Within an hour, both the FBI and DHS provided me with unfettered access to the actual cable outlining the threat. I continued to receive up to the minute briefings from the FBI over the next several days. This was critical as I had to continually make staffing and deployment decisions on a shift by shift basis. This shows that not only have we built strong relationships in the region, but more importantly the institutional structures that we have created are ensuring the flow of information. What was perhaps even more important was the quality of the information made available to me. The details in the briefings were far greater than law enforcement had received in the past and enabled me to focus our officers on the specifics of the threat.

Equally important, within 24 hours, the intelligence community collectively decided that the public needed to be informed of this credible threat, a significant departure from previous experiences. This decision helped law enforcement in several ways. For one, many of the actions of local law enforcement are much more visible than those of our federal partners, and in many cases are intended to be. In other words, our community members notice when we takes steps in relation to a heightened threat – they see us on the street, around critical infrastructure, and they know that something unusual is happening. Although this may only be a local concern, announcing the threat helps local authorities explain – and sometimes justify – our actions to the public. Local partners appreciate this support. More importantly, making this potential threat public helped us focus our community on reporting suspicious activity that may help us detect and deter those who may be interested in carrying out this threat. Obviously, when we can effectively harness and direct the attentions of the public, we can get more – and more useful – information to help us counter a threat. In this case, after the announcement our calls for suspicious activity jumped significantly.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01096 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.714

Most importantly, this announcement caused many of our private sector partners that had been involved in the joint briefings months earlier to report specific suspicious activity that warranted further investigation. For example, on September 10th, MPD was contacted by the general manager of a local hotel who advised that six males from various Middle Eastern countries had checked into the hotel between the 8th and the 10th. The last to arrive paid cash for his room, and asked for a specific view of a notable landmark. All six individuals placed "Do Not Disturb" placards on their doors.

A manager at another hotel contacted MPD on September 11th to report that cleaning personnel had found suspicious items left in a hotel room. The occupant had departed early without checking out, and leaving cash for the room. In this instance, the activity was linked to suspicious financial transactions reported earlier in the week. MPD and the FBI determined that the case did not have a nexus to terrorism, but was linked to criminal activity. Although neither instance was related to the 9/11 threat or to terrorism, the hotel managers took the right step in calling to report these indicators.

As you can see, providing some information to the public helps our efforts in the long run. It is a recognized principle in policing that sometimes you need to give a little information in order to get information. With the information about the threat on the anniversary of 9/11, and the visible government mobilization to it, the public is reminded of the importance of sharing information about suspicious activities with authorities. It reinforces the significance of the "See Something, Say Something" campaign, which is strongly supported by federal and local partners.

Fortunately, our experience here in the District of Columbia during the threats around the 9/11 anniversary highlighted several areas in which information sharing has improved. However, recognizing that my experience as the Chief of Police of the nation's capital may differ from other chiefs around the country, I reached out to colleagues around the country, including Commissioner Charles Ramsey, current Police Commissioner in Philadelphia and President of the Major City Chiefs. Across the board, Major City Chiefs agreed that the progress since 9/11 has been tremendous.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01097 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.715

One person simply and aptly described the fusion centers and the FBI's Field Intelligence Group as "game changers" for local police departments. We would not be able to prepare for and work together to prevent the significant threats facing our communities without this sea change in governmental cooperation. In addition to these cornerstones of federal—local information sharing, we continue to work on new links between the levels of government and with the private sector.

The Washington Regional Threat and Analysis Center, the District's fusion center, serves a critical role in receiving, vetting and sharing suspicious activity reports (SARs). The MPD receives SARs through many different methods, including 911 calls, text messages, email, our iWatchDC public web portal, from trained terrorism liaison officers, TRAPWire® reports from critical infrastructure sites, and observations made by patrol officers during the course of their duties. All of these SAR reports are forwarded to the fusion center and reviewed by trained analysts to ensure that the reports meet the established standards for suspicious activity reporting. If they do, the reports are entered into software programs where they are plotted for pattern analysis and proximity to critical infrastructure and other sensitive locations. The vetted reports are then entered into the National SAR Shared Space where they are available for review by the national network of fusion centers, and are forwarded to the FBI's eGuardian system for investigation by the Joint Terrorism Task Force (JTTF).

While the high tech support may be more interesting, low tech support is just as important. Our DHS partnership here in the District has been critical in educating the private sector about detecting and protecting business and customers from risks and threats. Even before the launch of the CVE working group, DHS has been a constant partner in trainings for the District's hospitals, hospitality industry, Business Improvement Districts, and others. They provide materials such as CDs and booklets that my Department would not be able to fund. Most importantly, they lend credibility to our public education efforts.

As we continue this forward progress, there are several areas that we should focus on. The most critical need continues to be effective and interoperable communications. Although the 9/11 anniversary highlighted the advances we have made in the past ten years, the earthquake that struck the region a few weeks earlier highlighted a problem we have not solved: instant

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01098 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.716

communications. When the earthquake struck, I was in a Drug Enforcement Administration briefing with two other police chiefs. For at least 15 minutes after it struck, we were not able to use our cell phones to communicate with anyone. Rest assured, we do have other options. We can use the Government Emergency Telecommunications Service (GETS), the decades-old failsafe communication procedure. We can, of course, also use police radios. But neither of these methods is efficient. Using the GETS card takes time, and, during emergencies, police radios will already be subject to increased traffic from the public calls for service. Neither of these is the answer for a secure and reliable communication network. From my perspective, the federal government must move forward with D-Block, a broadband spectrum for first responders. It is past time for this recommendation from the 9/11 Commission to be implemented.

Beyond that critical step, the overarching imperative is that we must continue to institutionalize this information sharing. If this process is just built on relationships and personalities, there will be gaps and it will ultimately fail. Most people in the federal community are excellent partners, but my colleagues around the country report that, to put it bluntly, some people and organizations still don't get it. More specifically, although progress has been made on over-classification, we must remain vigilant. It is particularly frustrating to local officials when major media outlets share more information than we have. It can't be an effective security strategy to have law enforcement learning of threats or other intelligence at the same time that the public and potential terrorists learn of it. Local law enforcement recognizes and respects that intelligence agencies are reluctant to reveal their sources or techniques. However we continue to believe the intelligence interests can be readily balanced with the need to share actionable intelligence. Although we share the same ultimate goal of safeguarding the country, both the law enforcement and intelligence community still need to work to understand the varying intermediate interests and operations of the other, in order to help each other more effectively and efficiently work to attain our organizational goals.

Maintaining robust fusion centers and co-locating analysts helps to counter any natural tendencies in the intelligence and law enforcement communities to operate in silos. This familiarity also helps the intelligence community to better target the information they share. There has certainly been progress in this area, but local law enforcement is still given more information than we can sift through. This brings us to one of the most critical issues facing local partnerships in homeland

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01099 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.717

security – funding. Nationwide, local law enforcement faces significant budget pressures, and police departments need federal support and resources to continue their vital work. This includes funding for fusion centers and analysts to work with law enforcement.

Although the technology to support homeland security efforts has advanced in areas many could not have foreseen a decade ago, we now eagerly look to future improvements. For instance, classified information is currently only available in specific locations, which requires that all organizations have representation at the right places. But public safety and homeland security is not a stationary effort. When there is a public safety threat facing a city, chiefs of police do not sit in a command center; we are out on the street, assessing conditions on the ground, directing our officers, and reassuring the public. While secure cell phones allow us some connectivity, we must find ways to share classified data on the move.

This would also help us with another gap: involving smaller jurisdictions in this effort. Although smaller jurisdictions have even fewer resources to devote to homeland security efforts than our major cities, our small cities and towns are just as likely to be the setting for suspicious and criminal activities. Larger police departments and the federal government bear equal responsibility for reaching out to and involving smaller law enforcement agencies. Regional fusion centers can fulfill a critical role by increasing outreach and technical assistance to smaller local law enforcement agencies. Every agency should have a trained Terrorism Liaison Officer able to connect their agency with regional and national efforts to detect and deter terrorist threats.

In closing, federal and local coordination in countering terrorism has advanced significantly over the past ten years. I know that the District, the National Capital Region, and the country are safer because of this work. However, we cannot rest as we still have work to do. I look forward to continuing to work with all of you on this vital effort.

Thank you again for the opportunity to appear before you today.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01100 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.718

STATEMENT FOR THE RECORD

Ronald E. Brooks, Director of the Northern California Regional Intelligence Center

Representing the National Fusion Center Association

United States Senate Committee on Homeland Security and Governmental Affairs

"Ten Years After 9/11: A Status Report on Information Sharing"

October 12, 2011

Chairman Lieberman, Senator Collins, members of the committee, thank you for holding this important hearing and for inviting the National Fusion Center Association (NFCA) to provide observations on the state of information sharing ten years after 9/11.

I am Ron Brooks, Director of the Northern California Regional Intelligence Center (NCRIC), one of our nation's seventy-two designated fusion centers, and Director of the Northern California High Intensity Drug Trafficking Area (HIDTA). I am a charter member of

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01101 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.719

the National Fusion Center Association (NFCA). I am a founding member and current Chair of the Criminal Intelligence Coordinating Council (CICC), and the Global Intelligence Working Group (GIWG), components of the Global Justice Information Sharing Initiative, a Federal Advisory Committee (FACA) established to advise the U.S. Attorney General on matters involving criminal intelligence and information sharing. I serve as the Chair of the State and Local Homeland Security and Law Enforcement Advisory Board for the Director of National Intelligence (DNI). I represent the CICC on the White House Interagency Policy Committee (IPC) on the Subcommittees on Fusion Centers and The Suspicious Activity Reporting Initiative. I also serve as the President of the National Narcotic Officers' Associations' Coalition (NNOAC), which represents 44 state narcotic officers' associations and more than 60,000 law enforcement officers.

Prior to my current assignment, I retired from the California Department of Justice as an Assistant Chief with the Bureau of Narcotic Enforcement. I have a total of thirty-seven years of service as a law enforcement officer with more than 30 of those years spent in narcotic enforcement and criminal intelligence assignments. Over the course of my career I have seen dramatic improvements in the ability and willingness of public safety agencies to share information. From the Regional Information Sharing Systems (RISS) that first enabled nationwide sharing of information among law enforcement 37 years ago and continue to be a cornerstone today, to the development of fusion centers after 9/11, we have come a long way.

The pace of information sharing progress has accelerated since 9/11, and sharing has improved even more rapidly in the last few years. Certainly there are challenges that remain, but there is good reason for optimism. The foundation has been laid, the path ahead is clear, and the commitment of a diverse set of stakeholders is encouraging. We must continue our commitment to a true nationwide information sharing enterprise with the National Network of Fusion Centers as a centerpiece and build on the success we have achieved to date.

Consider that just last month, less than 24 hours after high-level national intelligence regarding a 9/11-inspired threat was reported from a federal intelligence agency overseas, detailed threat information was sent through DHS and the FBI to the fusion centers and was put into the hands of local law enforcement. Fusion center analysts at the NCRIC, like those in many other centers were working around the clock, worked alongside FBI personnel to review suspicious activity reports and leads associated with the New York and Washington, DC threats, and to share actionable information with state and local public safety and private sector partners.

I think the average American assumes that this is the norm in all cases – and they ought to assume that. But those of us in law enforcement know how remarkable this example is, and how symbolic it is of the progress in information sharing that we have made in this nation since 9/11. The event demonstrated that the National Network of Fusion Centers plays a critical role in protecting the homeland and should be considered a national asset.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01102 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.720

The combination of revolutionary innovations in analytical and networking technologies, the lowering of cultural barriers to sharing, and the creation of trusted programs such as fusion centers has resulted in great progress. We must continue down the path we have created and remain tightly focused on reducing barriers and increasing trust.

Central to the continued improvement of information sharing is enhancement of the National Network of Fusion Centers, specifically the 72 state and major urban area fusion centers recognized by DHS. Fusion centers bring together law enforcement, public safety, fire service, emergency response, public health, protection of critical infrastructure and key resources (CIKR), and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities.

Fusion centers provide actionable intelligence to local, state, and federal decision makers who have the authority to allocate operational resources in terrorism and other investigations. I believe this is a key component of what fusion centers provide to our stakeholders. With public safety budgets and personnel stretched thin across the nation, actionable intelligence is even more essential to ensure diminished local and state resources are utilized as effectively as possible.

Fusion centers are owned and operated by state and local governments – not by the federal government – and yet they are national assets that are key to the nation's terrorism prevention strategy. This ownership and support structure enables fusion centers to be responsive to state and local needs as well as federal homeland security priorities. Mutual benefit is derived from the partnership between federal, state, local, and tribal stakeholders.

Federal support to fusion centers includes grant funding, assignment of intelligence analysts, technical assistance, training and exercises, linkage to key information systems, and security clearances. This federal support adds essential value to the resources committed by state and local governments to make the National Network a foundation of homeland security information sharing.

Consider these recent quotes and findings that indicate how important fusion centers have become in homeland security information sharing.

- **9/11 Commission Co-Chair Lee Hamilton** before the House Homeland Security Committee (September, 2011): "We have 72 fusion centers around the country [...]. They're of mixed, varied capacities, but they do bring together the right people in an area: state, local, and federal. They represent probably the best hope for giving you the kind of response you want on unity of effort in any given crisis."
- **Intelligence and National Security Alliance** (INSA) report (September, 2011): "In close cooperation with FIGs and JTTFs, fusion centers represent a foundation upon which to build a strong Homeland Security Intelligence Enterprise. Fusion centers are well-positioned to gather and share such information from state and local partners

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01103 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.721

across the Enterprise, particularly with JTTFs and FIGs. This type of information is necessary to pursue and disrupt activities that may be indicators of, or potential precursors to, terrorist activity. Likewise the FIGs are equally well-positioned to share transnational terrorist threat information with fusion centers. This example of connectedness facilitates a whole-of-government approach to protecting the public against terrorism."

- **Director of National Intelligence James Clapper** addressing the CSIS/INSA Domestic Intelligence event (September, 2011): "[Fusion centers] are the local nexus for imparting intelligence that we collect at the national level and [they convey upwards] street intelligence, which only state and local officials, I think, have good insight into. I have found [the State and Local Homeland Security and Law Enforcement Partners Board] to be a gold mine of wisdom and insight in an area I'm personally not as well-grounded on. And they made a very articulate, eloquent case for improving the intelligence enterprise domestically, and I think they are right on the money. And I intend to take that on."
- **The Homeland Security Policy Institute at the George Washington University**: Issue Brief on Leveraging Local Capabilities for National Counterterrorism Purposes (August, 2011): "Fusion Centers are the key to increased involvement by the local police. Not only do they have the resources desperately needed by local law enforcement, they have access to the traditional members of the intelligence community. The Fusion Centers should be the repository for each [local] agency's intelligence domains."
- **Secretary Janet Napolitano** addressing the National Fusion Center Conference (March, 2011): "[Fusion centers] allow frontline personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities."
- **2010 National Security Strategy of the United States**: "We will continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information; establish a nationwide framework for reporting suspicious activity; and implement an integrated approach to our counterterrorism information systems to ensure that the analysts, agents, and officers who protect us have access to all relevant intelligence throughout the government. We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information, conduct searches, and collaborate."

Fusion Center Contributions to Enhanced Information Sharing

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01104 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.722

The intent of public safety is to detect, disrupt, and prevent acts of crime and terrorism *before* they happen, and *if* they happen, to quickly identify and apprehend suspects and prevent further attacks.

To do this we need to constantly share appropriate information across jurisdictional and functional boundaries. In other words, we need to find the dots and then make sure barriers are lowered so they can be connected, even when one of us has a piece of information that no one knows is relevant.

Clear signs of progress in homeland security information are everywhere. Before 9/11, state, local, and tribal partners had little understanding of indicators and warnings of terrorism-related activity, and we rarely received warnings or threat information from the federal intelligence community. Today we are keyed into indicators, warnings, and threat information through a range of both FOUO and classified intelligence products in a timely manner.

Before 9/11, the intelligence community had no good way to receive pertinent information from state and local public safety, and there was very little direct communication with our federal partners regarding threat information. Today we routinely are sharing Homeland Intelligence Reports (HIRs) and Suspicious Activity Report (SAR) data with our federal partners and having direct dialogue via secure teleconferences with them to discuss specific threat information.

Before 9/11 at the state and local level we shared relatively few intelligence products among ourselves or with our federal partners, in part because we had no access to classified systems or information. Today more than 3,000 state, local, and tribal officers have security clearances that enable them to directly access to HSDN systems. These are remarkable changes in the past ten years; a true paradigm shift has occurred that has made our nation safer.

The information sharing environment has matured because partners have rolled up their sleeves and created solutions that are crossing boundaries efficiently. Strong leadership from the DHS Office of Intelligence and Analysis, the Office of the Program Manager of the Information Sharing Environment, the Bureau of Justice Assistance at the Department of Justice, the Nationwide Suspicious Activity Reporting Initiative's Program Management Office (NSI-PMO) and the Federal Bureau of Investigation has resulted in the strengthening of governance structures that are intended to lower barriers between Federal, state, and local organizations.

The National Network of Fusion Centers is critical in the facilitation of homeland security information sharing. Fusion centers receive, analyze, disseminate, and gather threat information with law enforcement and intelligence partners to help *prevent* attacks.

The concept is simple: when we can rapidly share threat intelligence among federal, state, local, and private partners and emergency operations centers, we are much better able to protect the public.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01105 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.723

Fusion centers have been key to achieving a "new normal" in homeland security cooperation after diligent efforts by countless federal, state, local, and tribal stakeholders. From where I stand, the difference between September 11, 2001 and September 11, 2011 is like night and day. Fusion centers are a major reason for the improvement, and it is critical to understand why.

Fusion centers have institutionalized collaboration against crime and terrorism among law enforcement, intelligence agencies, and other first responders. They enable more comprehensive analysis of information from a large number of sources for identification of patterns, trends, and anomalies. Technology and sharing agreements have made it easier to connect public safety partners. A fusion center analyst with single sign-on capability can search appropriate data housed in systems of other agencies. With these capabilities, fusion centers ensure that relevant information flows to agencies in a position to act, whether that is an FBI Joint Terrorism Task Force (JTTF), the Bridgeport Police Department, or the Maine State Police.

But fusion centers are more than information hubs. They embody a process – the *fusion process* – that has fundamentally changed how information is gathered, shared and transformed into useful intelligence at the local, state, and federal levels. It is about connecting the dots *and* putting national threat information in a local context. Fusion centers have taken steps to become "centers of analytical excellence" in order to ensure threat information is rapidly and accurately translated up or down the chain to public safety and intelligence partners for action. Training for analysts and direct contributions of analytical personnel from DHS have led to significant improvements in intelligence analysis capabilities across the National Network.

With this enhanced capability, a national intelligence enterprise is being created by connecting fusion centers, their information sharing and analysis partners, JTTFs, the HIDTA Investigative Support Centers, the RISS centers, major city and major county intelligence centers, the Nationwide SAR Initiative, and the Field Intelligence Groups (FIGs). This enterprise has been woven into a protective fabric for our nation, much the same way that the tightly woven threads of Kevlar form the ballistic vests that have protected my colleagues and me while we served to protect our communities.

This intelligence enterprise embraces the idea described in the White House Information Sharing Strategy of 2007 – that our nation's first responders are now our "first preventers." The International Association of Chiefs of Police (IACP) was spot-on when it said, "homeland security begins with hometown security." At the center of this new enterprise is the National Network of Fusion Centers' capacity to collaborate, connect, analyze, and share information.

There are significant efforts underway to address standardization of certain fusion center capabilities. Fusion center directors and the federal government have jointly worked to identify critical operational capabilities (COCs) for all fusion centers. The COCs relate to the ability to carry out four key activities: receive, analyze, disseminate, and gather information, all while

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01106 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.724

carefully adhering to privacy, civil liberties, and civil rights protections. Fusion centers have been successfully working to meet those capabilities, and the DHS Office of Intelligence & Analysis deserves great credit for proactively helping the centers in this effort.

Given the number of equities involved, the process is challenging, but tremendous progress has been made thanks to greatly enhanced collaboration between federal, state, and local stakeholders.

The Importance of Integrating State and Local Capabilities into Homeland Security Information Sharing

Prior to the terrorist attacks of 9/11, most of my colleagues in state, local and tribal law enforcement believed that the investigation of terrorism was the responsibility of the FBI and other Federal law enforcement and intelligence agencies. But as I watched the twin towers and the Pentagon burn while firefighters, police officers, and health workers ran toward the danger, and as I watched first responders race to a field in Shanksville, Pennsylvania, I realized that terrorism is a criminal act that threatens not only our way of life, but the communities that we have taken an oath to protect.

It became clear to many of us, whether at the International Association of Chiefs of Police, the National Sheriffs' Association, or the many other associations that represent the law enforcement profession that we needed to step up and do more to proactively prevent harm from being done to our fellow citizens. We were vividly reminded that *we* – state and local law enforcement along with other public safety and private sector partners – would be responsible for not only responding to these events and that we must take steps to prevent them.

It was not a matter of wholesale reorganization at the state and local levels. It was a matter of figuring out how we could use what we do every day – policing our communities and investigating crimes – to contribute to the larger homeland security mission. We are the front lines in our communities. Consider a few examples of local authorities encountering terror threats in the course of ordinary law enforcement:

- On the morning of December 14, 2007, three men pled guilty to federal terrorism charges. The Prosecutor described them as U.S. Citizens who had formed a radical Islamic terrorist cell while in prison and who planned to attack U.S. military installations, Israeli government offices, and synagogues in LA. Who uncovered the plot? It wasn't covert operatives in Afghanistan or federal agents conducting an investigation of Al Qaeda. It was local police officers investigating a gas station robbery in the Los Angeles suburb of Torrance, CA. During the investigation, officers found papers detailing the terrorist plot and shared them with the FBI. These terrorists were using money obtained from the robberies to purchase guns and other materials for their planned attacks.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01107 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.725

- In early 2006, the Duka brothers went to their local Circuit City store in Cherry Hill New Jersey to duplicate a video tape. The employee duplicating the tape saw that it depicted men in camouflage clothing firing guns and speaking in a foreign language. The store clerk notified local New Jersey police who brought in the FBI. Using an FBI informant, investigators uncovered a plot to attack and kill American soldiers at Fort Dix, New Jersey.
- Eric Rudolph, the Olympic Park bomber, who was also wanted for bombings of abortion clinics and the murder of a police officer, was arrested by a Murphy North Carolina police officer. That arrest resulted in the seizure of Rudolph's cache of weapons and 250 pounds of dynamite.
- On April 19, 1995, Oklahoma State Trooper Charles Hanger stopped Timothy McVeigh for no rear license plate. His arrest of McVeigh for an illegal firearm led to identifying him as the person responsible for bombing the Murrah Federal Building in Oklahoma City earlier that day. An attack that killed 168 persons including 8 federal law enforcement officers.
- A 2002 investigation by California Bureau of Narcotic Enforcement of a Canadian-based organization that was selling pseudoephedrine to Mexico-based methamphetamine producers was found to be a major source of funding for Hezbollah.

These examples demonstrate how state and local participation is central to a robust homeland security effort.

The increased focus on Countering Violent Extremism (CVE) recognizes the threat from individuals and small groups of people within United States borders. The national security enterprise must reach beyond the capabilities of the federal government and national intelligence community to identify and warn about impending plots that could impact the homeland, particularly when the individuals responsible for those threats operate within the United States and do not travel or communicate with others overseas. Effectively countering this threat from a public safety perspective requires the broadest possible integration of law enforcement resources and deep community engagement by state and local public safety agencies.

The new White House Plan for Empowering Local Partners to Prevent Violent Extremism in the United States recognizes this reality: "Government and law enforcement at the local level have well-established relationships with communities, developed through years of consistent engagement, and therefore can effectively build partnerships and take action on the ground." Local law enforcement has developed a good understanding of local norms through the community partnerships they have developed over time. They are more likely to identify anomalies and take action to prevent crime including a terrorism event from Homegrown Violent Extremists (HVE). Integration of this knowledge and with local and national threat intelligence is how those anomalies can come to light. Fusion centers are where that integration can and should take place. This does not mean that fusion centers should be the hub for community

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01108 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.726

engagement efforts, but rather that fusion centers are well-positioned to inform law enforcement about the HVE threat and to disseminate information to frontline personnel.

Many fusion centers have adopted an all-crimes approach. While the federal interest in fusion centers relates primarily to their ability to contribute to counterterrorism efforts, the reality is that the fusion process is effective for any public safety effort. Whether the crime is terrorism, child abduction, gang violence, or auto theft, the fusion process maximizes efforts to prevent, deter, or investigate the crime. Institutionalized collaboration through information sharing and co-location is effective no matter the nature of the crime.

Since more than 95% of crime in America is state and local, and since strained state and local budgets have meant significant reductions in public safety manpower, doing more with less is a must. One of the best ways we can accomplish this is by enhanced collaboration and information sharing through an all-crimes approach by fusion centers. The federal government benefits from the all-crimes approach because it amounts to "drilling" on real-world scenarios using the fusion center critical operational capabilities every day. When a terrorism threat emerges, fusion center participants and customers "know the drill."

"Tips and leads" has long been a familiar term in law enforcement. People call the authorities all the time to report activity they think is suspicious. Whether it is an unattended backpack in a shopping mall, suspected domestic violence in a neighbor's house, or an unfamiliar person hanging around a playground, citizens report tips and leads with the expectation that law enforcement will respond and investigate the suspicious activity. The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is an effective way to gather and analyze "tips and leads" on a broad scale for analysis of suspicious activity that might be linked to terrorism.

NSI is a key to linking state and local public safety and the federal homeland security enterprise. A study recently conducted by RTI International and released by the Institute for Homeland Security Solutions found that nearly a quarter of terrorist plots were uncovered during investigations of crimes not related to terrorism. NSI recognizes this reality and ensures that we are better trained and connected to recognize and share possible threat information.

The NSI facilitates the appropriate sharing of observed suspicious activity between state and local public safety and federal counterterrorism authorities. The SAR system has been greatly enhanced by the work of the fusion centers through the Terrorism Liaison Officer (TLO) and Fusion Liaison Officer (FLO) networks that fusion centers have established. It is the National SAR Front Line Officer Training and constant interaction between the fusion centers and their liaison officers, along with the indicators, warnings and bulletins passed to them by the fusion centers that has greatly enhanced our national capacity for reporting suspicious activity.

In just the past three years, California's fusion centers have provided beginning, intermediate, and/or advanced TLO training to more than 32,000 law enforcement officers and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01109 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.727

other first responders at more than 700 fusion center sponsored classroom trainings. California's fusion centers have a current cadre of more than 7,000 TLOs but we have trained many more officers and first responders in TLO concepts and in the indicators and warnings of terrorism, since all first responders who interact with the community may be in positions to observe suspicious activity. My own fusion center, the NCRIC, reaches more than 8,000 public safety professionals throughout our fifteen county region each time we send out a bulletin, officer safety alert or request for information.

Equally important is identifying the infrastructure, key resources and other vulnerable targets including those in the eighteen DHS designated sectors and those that may not fit within the DHS sectors but that may be important or vulnerable. In my fusion center we have identified and geospatially mapped all of the DHS-designated critical infrastructure and other locations such as military recruiting stations, schools, general aviation facilities, firearms and chemical dealers that have been deemed valuable or vulnerable to attack. This was a major effort by our fusion center and has led to the cataloging of more than 7,000 sites. This is critically important because the key to preventing or disrupting an act of terrorism is to understand the threat, know what infrastructure may be targeted and identifying when a threat or suspicious activity intersects critical or vulnerable infrastructure. I know that California's experience is similar to that of most fusion centers throughout the nation in this regard.

Without the National Network of Fusion Centers, there would not be an organized hub to request or share information regarding terrorism, trans-national criminals, violent gangs, drug trafficking organizations and other organized crime. More importantly, there would not be a portal to the SAR process or a system to promote the sharing of information or requests for information (RFI) between the FBI, DHS I&A, and local public safety entities.

The concept of "Intelligence Led Policing" has been developed to ensure state, local, and tribal authorities are fully leveraged to contribute to the homeland security mission. This concept is not meant to turn police officers into Jack Bauer. It does not suggest that cops should spy on our fellow citizens. It describes the obvious: that law enforcement officers should continue to do what they have always been trained to do – identify suspicious activity, report that activity, and prevent crime – while at the same time respecting the privacy rights and civil liberties of fellow citizens.

Fusion centers have enhanced state and local operational coordination with the FBI. For example, every fusion center gives the FBI – via existing linkages with Joint Terrorism Task Forces – a first look at every suspicious activity report (SAR). The FBI can decide to pursue the SAR under their authorities; in most cases they decline and the fusion center can validate the SAR as worthy of pushing to the Information Sharing Environment, determine that the SAR is not terrorism (i.e., narcotics related), is constitutionally protected activity, or is not valid for some other reason.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01110 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.728

Thanks to fusion centers we are sharing *more* information *more effectively* than ever before. This is happening despite the fact that no single entity has the authority to enforce effective information sharing practices. Because of the decentralized nature of public safety, policies on sharing information cannot be dictated by any one organization. Common policies and practices must be developed by consensus and continually reinforced through real engagement. As you might imagine, this is extraordinarily difficult to achieve in practice. Yet, the public expects that we do it, and from my vantage point the public has reason to be proud of what we've done. Fusion centers have institutionalized information sharing among a broad range of local, state, and federal stakeholders.

Whether the information handled by a fusion center is criminal or terrorist in nature does not matter. It certainly doesn't matter from a citizen's perspective. There was no fusion process in place to tie a Maryland State Trooper's routine I-95 traffic stop of 9/11 hijacker Ziad Jarrah on September 8, 2001 with information in federal databases about Jarrah's previous suspicious activity related to terrorism.

Since fusion centers are owned and operated by state and local entities, there is wide variation among the centers in terms of budget and capabilities. Fusion center priorities in Tennessee are different from priorities in New York State and from our center in the San Francisco Bay area. The interests are different because their populations are different, and the fact that they are free to address the issues they feel need addressing is a strength of the national network of fusion centers.

The common thread through all the centers – and the key federal interest – is a link to federal partners and to each other through information sharing mechanisms. The critical operational capabilities of each center will ensure the centers are ready and able to support homeland security missions regardless of their local priorities.

This year, fusion center directors have worked with DHS Intelligence and Analysis to develop and implement cost and operational assessments. Fusion centers are in the process of reporting through this assessment detailed budget data including the mix of federal, state, and local resources contributed to the centers. While fusion center directors understand the imperative to measure effectiveness of the centers, Congress should understand that the federal government cannot unilaterally impose a performance management program upon fusion centers because they are owned and operated by state and local governments. The NFCA is in full agreement with the 2010 GAO report recommendation that the value fusion centers provide to the Information Sharing Environment must be demonstrated as part of sustainment funding justification. We are working together and with our federal partners to develop performance measures which demonstrate that value.

Budget support for fusion centers varies widely. To give you a sense of the diversity, some centers are almost entirely funded with federal grant dollars while some are almost entirely

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01111 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.729

funded with state dollars. Yet in all cases, state and local agencies contribute full-time personnel to their centers, and those contributions are generally not accounted for in the centers' budgets.

It is important to understand that if federal support for fusion centers declines in coming years, many fusion centers that are mostly supported with federal resources could shrink or disappear. The impact on national homeland security information sharing would be serious: if nodes in the national network shut down there is no clear way to integrate the decentralized information and local knowledge into the federal homeland security enterprise. The NSI, among other initiatives, would become much more difficult to implement on a wide scale.

In other words, the nation's counterterrorism capabilities would be eroded, and forward progress would be reversed.

While each center is unique, they are making progress toward the achievement of certain critical operational capabilities that are standardized across the national network. For example,

- Privacy policies have been established across all 50 States and all operational fusion centers at least as comprehensive as the 2006 Information Sharing Environment (ISE) Privacy Guidelines.
- Training has occurred for more than 200,000 local, tribal, state, and federal front line officers to identify and report suspicious activity in accord with the ISE SAR Functional Standard v1.5, and several thousand analysts have been trained in accord with vetting guidelines to ensure that ISE SARs are demonstrably behavior-based and their handling (retention, redress, and other related considerations) are fully compliant with privacy policies.

There is a specific and unique space for the information and sources "owned" by state, local, and tribal public safety agencies. Federal, state, and local policies should therefore ensure that this space is supported with the most professional and effective criminal and homeland security intelligence operations possible. That is how we ensure that state and local capabilities are fully leveraged to protect the homeland.

It is widely recognized that whole-of-government counterterrorism efforts require a decentralized, distributed system, as called outlined in the Markle Foundation report and the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). This system allows for local control within a national policy and mission context. The National Network of Fusion Centers – owned and operated by state and local governments with deep support and partnership from federal agencies – is a stark embodiment of this model.

This decentralized, distributed system is effective as long as appropriate information is widely shared or made available for others to analyze. At the core of agencies' willingness to share information is *trust*. With more than 18,000 law enforcement agencies staffed by more than 840,000 law enforcement officers, more than 30,000 fire departments staffed by more than

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01112 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.730

1,000,000 career and volunteer firefighters, 50 state governors, countless critical infrastructure security professionals, public health workers, and emergency medicine workers, and the dozens of federal law enforcement and intelligence agencies in the United States, we need trusted mechanisms where institutionalized collaboration can take place on a regular basis.

Building that trust requires time, financial investment, commitment, and repetition. The National Network of Fusion Centers is the connective tissue that creates a trusted bond and fosters effective working relationships among tens of thousands of agencies and organizations with millions of public safety employees.

Several developments have been responsible for many of the major improvements in information sharing from the state and local perspective:

- The Criminal Intelligence Coordinating Council (CICC) and Global Intelligence Working Group (GIWG) are where much of the hard work has been done over the past decade to develop and create consensus around key information sharing principles among local, state, and federal public safety.

- Global and the CICC are critical because they focus on the development of documents that have the force of national policy and are widely adhered to. Global and the CICC have facilitated the development of the National Criminal Intelligence Sharing Plan, Law Enforcement Analytic Standards, technical data exchange standards, Fusion Center Privacy Policies, Fusion Center Guidelines, Baseline Capabilities for Fusion Centers, and have contributed to the National Strategy for Information Sharing, among other important initiatives.

- This institutionalized collaboration is what we need to ensure the continued commitment and building of trust among the greatest possible number of stakeholders.

I cannot overstate the importance of having the Attorney General's core advisory groups - Global and the CICC - represented within the White House's capstone governance body for information sharing. In addition to advising the AG, they have become primary engagement points with the Secretary of DHS, the Director of National Intelligence, and the White House national security apparatus. This type of access deepens and strengthens connectivity to the larger enterprise and ensures solutions are truly whole-of-government.

The many individuals involved in these efforts go unnoticed and unappreciated, but they deserve a lot of credit for leading us to where we are today.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01113 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.731

Recommendations for Improvement

Homeland security partnerships through DHS state and local assistance programs need to be preserved and strengthened *with a focus on prevention.* After 9/11 much of the federal assistance to state and local partners was on supporting enhancements to *response* capabilities. It is time to invest those resources in enhancements to *prevention* capabilities in a more focused way. This is even more critical in a time of declining budgets at every level of government. The number one responsibility of government at all levels is to protect citizens. We must vigilantly guard against the loss of prevention and deterrence capabilities, including fusion center capabilities. In fact, to appropriately reflect the role fusion centers play in prevention, the National Network of Fusion Centers ought to be included in the Prevention Framework called for in Presidential Policy Directive 8 (PPD-8).

Information gathering, analysis, and sharing to protect the homeland cannot improve if resources are not there to support the bodies, technology, and training. The State Homeland Security Grant Program (SHSP) and Urban Area Security Initiative (UASI) provide critical support to enable fusion center operations. The Implementing the 9/11 Commission Recommendations Act of 2007 required that 25% of SHSP and UASI funds be used for law enforcement terrorism prevention (LETP) activities. Congress should take steps to ensure that funds directed toward LETP activities are truly applied to *prevention* activities such as fusion centers.

Severe reductions in funding for the UASI and SHSP over the past year and the additional deep anticipated next year will threaten the existence of some fusion centers. Without that support, the strong federal-state-local partnerships that have been carefully built over the past 10 years would begin to be dismantled.

State and local public safety budgets have been severely cut back across the country in recent years. The top priority of these agencies is always hometown security, and reduced budgets mean that without federal support, the ability to contribute to the larger homeland security mission is significantly reduced. If Congress, DHS, DOJ, and our other federal partners expect to continue to benefit from full participation of state and local public safety, then federal investment through these programs must continue to be robust.

Long-term sustainment of the National Network of Fusion Centers is a shared responsibility among all levels of government and is critical to ensure advances in information sharing are preserved and expanded. Sustainment means a long-term commitment of targeted federal support through effective legislative authorization and adequate annual appropriations for programs that contribute value to fusion centers and allow them to serve as the foundation for a strong Homeland Security Intelligence Enterprise. Sustainment includes not only financial support, but also the contribution of intelligence analysts, providing training for fusion center personnel, and ensuring secure access to appropriate federal information systems.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01114 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.732

State and local commitment to sustainment is also essential. This includes enhanced collaboration between fusion centers and state homeland security advisors (HSAs) as well as local, tribal, county, and regional authorities. It also means the commitment of state and local agency personnel to fusion centers. A commitment to long-term sustainment will allow fusion centers to achieve and maintain the critical operational capabilities, which ensures both state and local jurisdictions and the federal government derive benefit from the investment made in building and strengthening the National Network of Fusion Centers.

Certain types of information and intelligence developed at the federal level are still not being shared effectively with state and local entities. To ensure state and local public safety is best able to contribute to homeland security, trusted forums for development of information sharing policies and practices must be supported. This includes at a minimum the support of fusion centers, the GIWG, CICC, the Nationwide SAR Initiative at the Department of Justice, and the DHS Office of Intelligence and Analysis.

With President Obama's release last week of an Executive Order regarding the security of classified information, the scope of the Information Sharing Environment has expanded to include sharing and safeguarding of this information. State and local stakeholders are just as concerned about the shared vulnerabilities exposed through the Wikileaks incident, and we welcome participation in efforts to ensure responsible sharing of classified information. It is gratifying to see the focus on strengthening governance and common solutions, and I believe the leverage of the Program Manager for the ISE is a core part of the way forward.

Joint Terrorism Task Forces (JTTFs) play the lead role in counterterrorism investigations. Owned and operated by the FBI with close cooperation and participation by state and local partners, JTTFs are key "customers" of fusion center analytical products. The National Network of Fusion Centers also supports the dissemination of information from JTTFs to the broader public safety community. Fusion centers do not duplicate the functions of JTTFs, and JTTFs are not organized to achieve the missions of fusion centers. The two programs are complementary and both are essential to effective homeland security information sharing and investigations. Congress should ensure both efforts are fully supported.

JTTFs deal primarily with terrorism and other criminal matters related to various aspects of the counterterrorism mission. Fusion centers generally take an all-crimes approach and deal with criminal, terrorism, and other public safety matters across multiple disciplines. JTTFs primarily conduct terrorism investigations and share intelligence with law enforcement and homeland security agencies as appropriate. Fusion centers analyze and assess local implications of national threat information and produce actionable intelligence for dissemination to public safety stakeholders in their area of responsibility and beyond. In short, the missions are complementary and essential, and they do not overlap.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01115 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.733

Conclusion

The rapid stand-up of a National Network of Fusion Centers with such an important mission and so many stakeholders means that growing pains are inevitable. Tough lessons have been – and will continue to be – learned. It is easy to focus on mistakes when they are made, and we will unfortunately not be able to stop 100% of the threats to our country. Yet the organic grass-roots development of this decentralized National Network is a tremendous accomplishment. It was born from the dedication of the hundreds of thousands of public safety personnel across this nation and has become a true national asset.

We are sworn to protect the public. Yet the public – and Congress – will never know about the majority of the successes we have on a daily basis. The information and intelligence sharing mechanisms we have developed since 9/11 – including fusion centers – have helped immensely. They must be nurtured and have the full support of Congress so that homeland security information sharing can be continuously improved.

On behalf of the National Fusion Center Association, we commend your long-standing commitment to effective information sharing and respectfully ask for your continued support. Thank you for the opportunity to provide our views on this important issue.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01116 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.734

APPENDIX: Examples of Fusion Center Effectiveness

(Source: http://www.dhs.gov/files/programs/gc_1296488620700.shtm)

1) Fusion Center is Instrumental in the Arrest of an Attempted Bombing Suspect

Colorado Information Analysis Center, June 2011

In June 2011, the Lakewood, Colo. Police Department received information that an individual had placed two improvised explosive devices at a Borders book store at the Colorado Mills Mall. Due to the nature of the crime, the Lakewood Police Department notified the Federal Bureau of Investigations (FBI) of the incident, who in turn activated the Joint Terrorism Task Force (JTTF). The JTTF and Alcohol, Tobacco, and Firearms Agents responded to the scene and began collecting information which they passed to the Colorado Information Analysis Center (CIAC). A few hours later, the Colorado Information Analysis Center (CIAC) sent information to fusion centers nationwide and Terrorism Liaison Officers (TLO) statewide, requesting information that may relate to the incident. Less than 15 minutes after this information was sent to Colorado TLOs, the CIAC received vital information from a State Trooper. About 24 hours earlier the suspect had crashed his vehicle and was taken into custody for Felony Menacing and Driving Under the Influence of Alcohol. After receiving the information from the CIAC, the arresting officer believed the suspect he arrested was also the suspect in the book store bombing attempt. Concurrently, and while the investigation was still active, the CIAC received another lead from a different TLO which linked the suspect to yet another device that partially detonated near a hotel a short distance from the book store. The CIAC in turn passed this information to the FBI JTTF to further support the investigation. The suspect is being held on charges stemming from the incident.

2) Intercepting a Suspicious Trailer Headed to Times Square

Multiple Fusion Centers, October 2010

On October 8, 2010, an advisory was sent out by the New York Police Department concerning a suspicious tractor trailer whose driver reportedly diverted its route to Times Square in New York City in exchange for $10,000. The deployed Department of Homeland Security (DHS) Intelligence Officer (IO) in New York informed several fusion centers in the affected area. Subsequently, the Rhode Island Fusion Center discovered that the original owner of the truck was a California native and asked the Northern California Regional Intelligence Center to run a background check based on the owner's information. Within two hours of the advisory's release, information from these two fusion centers was used to coordinate with the Connecticut Intelligence Center, which enabled Connecticut State Police to locate the tractor trailer before it reached its reported target in New York City. The Connecticut State Police searched the vehicle and questioned the driver and passenger.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01117 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.735

Ultimately, officials concluded that the vehicle was not a threat, but the fact that these fusion centers, supported by Department of Homeland Security IOs, were able to turn this incident from a Suspicious Activity Report (SAR) to resolution in a matter of three hours shows the value of the National Network of Fusion Centers.

3) Fusion Center Provides Critical Information in Arrest of Suspect on Kidnapping and Rape Charges

Multiple Fusion Centers, August 2010

The Pennsylvania Criminal Intelligence Center (PaCIC) provided information regarding the abduction and rape of a woman in Mead Township, Pennsylvania, in its August 3, 2010, daily intelligence summary, which included a description of the suspect as well as his Maine license plate number. Because the suspect had an out-of-state license plate, a fusion center analyst at the PaCIC provided the product to the Maine Intelligence Analysis Center (MIAC) along with details on the case. Based on this coordination, the Maine State Police determined the suspect had fled the United States for Canada. Working with the Royal Canadian Mounted Police in New Brunswick, Canada, the suspect was found and arrested on charges of kidnapping and rape.

4) Fusion Centers Provide Critical Information to Faisal Shahzad Case

Multiple Fusion Centers, May 2010

After the attempted bombing of Times Square by Faisal Shahzad, fusion centers across the country shared tips and leads directly pertaining to Shahzad with the Federal Government. Florida Fusion Center analysts discovered Shahzad was associated with two subjects that had previously resided in Florida. Pertinent information was passed to the Federal Bureau of Investigation (FBI) Joint Terrorism Task Force (JTTF) to further pursue leads. The JTTF provided the information to the National Counterterrorism Center, which used the information in a subsequent intelligence product.

In New York, an alert AAA employee filed a SAR with the New York State Intelligence Center regarding a call on May 2, 2010 – when Shahzad called for assistance because he had locked his keys inside the vehicle. This was the same vehicle later recovered at the airport with a firearm inside on the day Shahzad was arrested. This information was forwarded to the FBI to support investigation and corroboration.

5) Fusion Center Supports Tribal Drug Investigation

Arizona Counter Terrorism Information Center, May 2010

The Arizona Counter Terrorism Information Center supported a five-month investigation led by a tribal partner, the Tohono O'odham Nation (TON) Police Department and the Bureau of Indian

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01118 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.736

Affairs (BIA) Division of Drug Enforcement. This investigation led to the arrest of 10 suspects and the apprehension of weapons, cash, vehicles, cocaine, marijuana, and ecstasy – the largest drug enforcement operation in TON history. The investigation marked a key opportunity to collaborate with tribal partners and opened information sharing initiatives between several other agencies, including the FBI, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and other police departments in the area.

6) Fusion Center in Colorado Supports Investigation of Woman Arrested on Terrorism Charges

Colorado Information Analysis Center, March 2010

In September 2009, the Colorado Information Analysis Center (CIAC) supported an investigation of a local missing woman whose mother indicated that her daughter had converted to Islam through the Internet and had been communicating with a man from Pakistan. The CIAC was alerted that the missing woman, Jamie Paulin-Ramirez, was possibly traveling to New York to meet the man. Upon analysis of this report, the CIAC provided this information to the local JTTF. The information supplemented an open FBI investigation on the woman.

Paulin-Ramirez was later linked to Colleen R. LaRose (Jihad Jane), who was charged in March 2010 with terrorism-related crimes, including conspiracy to commit murder and providing material support to terrorists. Subsequent news reports indicated that suspected terrorist Najibullah Zazi, who pleaded guilty in February 2010 of planning to bomb the New York subway system, may have also been in contact with Paulin-Ramirez via the Internet.

In March 2010, Paulin-Ramirez was detained in Ireland with five others in connection with a terrorist conspiracy to kill a Swedish cartoonist who had portrayed the prophet Muhammad as a dog in a cartoon. The CIAC cooperated with the FBI to provide further information from their prior analysis of information pertaining to Paulin-Ramirez.

7) Fusion Center Supports Zazi Investigation

Colorado Information Analysis Center, September 2009

In the Najibullah Zazi case, the CIAC provided analytic support to the Denver FBI and the Department of Homeland Security regarding the suspicious activity reported to the CIAC through the public website and 1-800 number. In support of this effort, the CIAC provided personnel to assist the Denver FBI in the investigation and support the field operations. CIAC analysts also assisted in the review and analysis of the evidence obtained during the execution of the search and arrest warrants. CIAC leadership addressed media inquiries regarding the investigation, the threat to Colorado residents, and the threat to national security.

8) Fusion Centers Support the G-20 Summit

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01119 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.737

Multiple Fusion Centers, September 2009

The Department of Homeland Security worked with federal, state, local, and private sector partners, including the five surrounding fusion centers, in support of the G-20 Summit held in Pittsburgh September 24-25, 2009. The Department leveraged open source materials and information received from fusion centers to support federal, state, and local partners in making informed decisions and understanding the threat environment. The Department also deployed six analysts from headquarters to provide intelligence support to the three G-20 Pittsburgh Summit Command Centers. Participation by partners at all levels of government enabled leadership to maintain situational awareness of the event and receive timely, relevant information.

9) Fusion Centers Coordinate Security for 2008 Republican and Democratic National Conventions

Multiple Fusion Centers, July 2008

Two fusion centers, the Minnesota Joint Analysis Center (MNJAC) and the CIAC, supported information sharing with state and local entities for the 2008 political conventions. For the Republican National Convention, the MNJAC provided 24/7 support to facilitate information and intelligence sharing to the Principal Federal Official's support cell. For the Democratic National Convention (DNC), the CIAC coordinated state and local input to the Special Events Working Group and developed a Joint DNC Threat Assessment. As part of this effort, the CIAC and the FBI jointly managed the Intelligence Operations Center (IOC), which was responsible for collecting, fusing, analyzing, de-conflicting and disseminating all information in support of DNC security operations. The CIAC also served as the primary conduit for sharing DNC information with state and local entities.

10) Fusion Center Supports Bomb Threat Case

Central California Intelligence Center, May 2008

The Central California Intelligence Center (CCIC) coordinated with its co-located JTTF in a case that resulted in the May 2008 federal grand jury indictment of two men charged with making bomb threats to Delta Airlines and the U.S. Embassy in Italy. Intelligence analysts at the CCIC provided relevant background to enable JTTF agents to interview the subjects. Both men were charged with one count of making a hoax threat under Section 1038(a) of Title 18. One defendant was also charged with threatening to destroy an aircraft, and the other was charged with making a threat to destroy a building with explosives. The former pled guilty in May 2009 and was sentenced to 36 months probation; the prosecution of the latter defendant was deferred in March 2009 for 18 months while he participates in a program of psychiatric treatment.

11) Fusion Center Support Prevents an International Kidnapping

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01120 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.738

Central California Intelligence Center, May 2008

In May 2008, the CCIC played a key role in disrupting the attempted kidnapping of a three year-old child. The Department of Homeland Security deployed IO in Sacramento coordinated with the CCIC Director and a Sacramento County Sheriff's Office Task Force Commander on an Amber Alert for the child, noting the suspect was wanted for rape and murder and had intentions to leave the country. Coordinating with the Department of Homeland Security National Operations Center (NOC), local law enforcement, and Interpol, the CICC and the Department IO were able to track the suspect and the kidnapped child to a flight bound for the Netherlands. With only hours to spare, the Department deployed IO coordinated with authorities to ensure law enforcement in Amsterdam detained the subject. As a result of this effort, the child was found unharmed.

12) Fusion Center Aids in Preventing "Virginia Tech Style" Attack

Multiple Fusion Centers, January 2008

In January 2008, the Illinois Statewide Terrorism and Intelligence Center (STIC) received information that a Virginia man had claimed to be traveling to the University of Illinois to kill a female subject and her boyfriend and carry out a "Virginia Tech style" shooting on the university campus. The STIC, in cooperation with the Virginia Fusion Center, produced and disseminated an Intelligence Alert to hundreds of state and local law enforcement officers nationwide within two hours of the initial notification. The Virginia State Police, working with local law enforcement, located and detained the suspect the next day. The FBI subsequently adopted the case, and the subject pled guilty to five counts of transmitting in interstate commerce and communications threatening to injure the person of another. The subject was sentenced to 48 months in prison and will serve three years supervised parole.

13) Fusion Center Supports Goose Creek Case

Florida Fusion Center, August 2007

On August 4, 2007, the Department of Homeland Security deployed IO assigned to the Florida Fusion Center (FFC) received a call from the Florida Homeland Security Adviser (HSA) regarding an on-going traffic stop of two University of South Florida students in Goose Creek, South Carolina. The HSA didn't have specifics other than it involved a bomb squad and a Florida registered vehicle. The Department of Homeland Security NOC had no visibility of the traffic stop, but began to query North Carolina and South Carolina. The Department deployed IO received further information regarding the incident from an FFC representative with specific information he received from a colleague at Operation SeaHawk in South Carolina. The FFC was able to provide the tag number of the vehicle and conducted full database checks on the vehicle's history and owner information.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01121 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.739

All of the results were provided to the NOC, South Carolina, and Tampa-JTTF within minutes for their situational awareness. The FFC was able to provide full database checks on the subjects to South Carolina and Tampa-JTTFs.

An indictment was unsealed August 31, 2007, against the two students, Ahmed Abdellatif Sherif Mohamed and Youssef Samir Megahed, both Egyptian nationals, charging them with transporting explosives in interstate commerce without permits. Mohamed was also charged with distributing information about building and using an explosive device. Mohamed pled guilty to providing material support to terrorists on June 18, 2008, and was sentenced to 15 years in prison December 18, 2008. Megahed was acquitted of explosives charges in April 2009. Immigration and Customs Enforcement later took custody of him and launched removal proceedings against him. An immigration judge declined to find Megahed removable and granted his Motion to Terminate on October 9, 2009. The Department decided not to appeal the judge's order.

If it were not for the fusion centers and an Operation SeaHawk representative, Florida and the Department would not have gained situational awareness regarding the incident. Florida was able to provide relevant information regarding the subjects and associates to South Carolina law enforcement officials and the JTTF within minutes to aid in their investigation.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01122 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.740

Statement of Zoe Baird Budinger[1] and Jeffrey H. Smith[2]
Senate Committee on Homeland Security & Governmental Affairs

October 12, 2011

Ten Years After 9/11: A Status Report On Information Sharing

Thank you Chairman Lieberman and Senator Collins for holding this hearing and for your leadership on this critical issue. This statement is submitted on behalf of the Markle Task Force on National Security in the Information Age.

We commend the Committee for the significant time and energy you have devoted to making homeland security information sharing a top national priority. You have led this effort since the attacks of 9/11 with a singular commitment and have helped make this nation safer. Since 2002, the Markle Task Force has provided policymakers, including this Committee, with recommendations[3] to help accelerate our government's use of information and information technology to better understand the threats we face and make better decisions about those threats, while protecting traditional civil liberties. Our ultimate goal has been to help enable the federal, state, and local governments to work together to protect our nation from terrorism and other threats.

A substantial change has occurred throughout government in the way security professionals do business. Information sharing has become more widespread and the government has made real changes that are necessary to respond to new threats. That said, progress has been too slow in some places and has lacked adequate guidance or oversight in others.

In the decade since the September 11th attacks, our government has answered the threat of terrorism by transforming itself in important ways. The lack of major attacks on our homeland over the past decade, along with a string of notable intelligence successes, including the recent strikes on Anwar al-Awlaki and Osama bin Laden, is a testament to the fact that things have changed. It has been hard to do, and there is much more to be done, but there has been real progress that deserves to be acknowledged.

The attacks on 9/11 showed all of us that the Cold War "need to know" system for managing classified and sensitive information drove a culture of information security that resulted in countless stovepipes and secretive pockets of the nation's most valuable information. It may have worked in the Cold War, but it was not adequate to keep America safe in a world of asymmetric threats. Many realized that protecting America in this new threat environment would require the government to operate in an entirely new way.

You have enacted two major laws that have substantially changed how government understands those who would do us harm and how it acts to prevent that harm. We have tried to contribute to this challenge. Over the course of four reports written between 2002 and 2009,[4] the Markle Task Force

---

[1] Zoe Baird Budinger is President of the Markle Foundation. She and Jim Barksdale co-chaired the Foundation's Task Force on National Security in the Information Age. She served on the President's Foreign Intelligence Advisory Board from 1993–2001 and the Department of Defense: Technology and Privacy Advisory Committee ("TAPAC") from 2003–2004.

[2] Mr. Smith is a member of the Markle Task Force on National Security in the Information Age and a Senior Partner at Arnold & Porter LLP. He is a former General Counsel of the Central Intelligence Agency and currently serves on the Director of CIA's External Advisory Board. Mr. Smith will provide today's oral testimony.

[3] For more information on all of our previous work on information sharing, please visit www.markle.org/national-security.

[4] All of the Markle Task Force reports are available at http://www.markle.org/national-security/markle-task-force-national-security/reports.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01123 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.741

grappled with how the government could operate in a new way. With national security experts from every administration since President Carter, civil liberties advocates, information technology executives, academics, and many from within government and the Intelligence Community, we proposed a collaboration across agencies that would foster a robust sharing of information and ideas. In order for this collaboration to be successful a set of policies was required that would simultaneously empower and constrain government officials by making clear what collection, analysis, sharing, and uses of information were permissible, and what were not. Instead of storing data centrally, we suggested storing data on a distributed network, thus eliminating the gaps between government agencies and empowering all players in the network—including those at the edges—to create and share actionable and relevant information. Such a network is more protective of civil liberties because it avoids a focus on creating large centralized databases and limits access to information to those who appropriately should use it. The objective of this network was to enhance the government's ability to discern indicators of terrorist activity amid overwhelming amounts of information and to create more time for the nation to respond to threats more effectively.

Since 9/11, there has been a shift in federal and state government culture towards this type of information sharing and collaboration model, and some segments of the government have made progress implementing information sharing policies. Government sources report that this approach, in turn, has been very successful. The agility that sharing information has given our government officials has enabled them to better understand our rapidly changing world. If information sharing policies and practices had not been implemented, these successes might have been tragedies. Clearly, now is not the time to turn back the clock on information sharing.

Of course, there are risks inherent in sharing more information, but these risks are outweighed by the risks of not sharing. The attacks on 9/11 are a stark example of this.

We would like to briefly discuss: (i) where we were ten years ago, (ii) where we are now, (iii) where we fall short, and (iv) where we should be going. The Markle Task Force has four concrete recommendations for further improving information sharing and continuing this post-9/11 transformation. We hope our comments will give the Committee a better sense of how far the government has come and what steps still need to be taken.

I. Where We Were Ten Years Ago: *Failure to Adapt to a Networked World*

In hindsight, it is clear that our failure to discover the September 11th plot was in many ways a failure of information sharing and a failure to empower our best and brightest. It was a disastrous illustration of our government's failure to adjust to a networked world. The U.S. government might have prevented the 9/11 attacks if the Federal Bureau of Investigation ("FBI"), the Central Intelligence Agency ("CIA"), and state and local law enforcement had connected what they each knew about the hijackers and acted upon it.

Ten years ago, our law enforcement and intelligence communities were driven by a Cold War "need to know" culture that stovepiped information and stymied cooperation. As demonstrated by the ten lost "operational opportunities" to derail the September 11th attacks that the 9/11 Commission identified, both the CIA and the FBI failed to disseminate information in the run-up to the attacks. This was, in part, because of the so-called "Wall" between law enforcement and intelligence. What information they did share often lacked the full context that might have shed light on its big picture significance. The culture that led to this failure is vividly illustrated by a CIA analyst who told the 9/11 Commission that he did not volunteer information he knew about a suspected terrorist when the FBI showed him surveillance pictures of the individual because he "was not authorized to answer FBI questions regarding CIA information."[5]

Silos also existed between agencies and within individual agencies that forced people to work in

[5] Thomas H. Kean et al., The 9/11 Commission Report 269 (2004).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01124 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.742

hierarchical pyramids, preventing people on the edges of the system from collaborating to chase down leads. For instance, in July 2001, an FBI agent in the Phoenix Field Office prepared a memo on the "possibility of a coordinated effort" by Osama bin Laden to send students to civil aviation schools. A month later, the FBI's Minneapolis Field Office initiated an unrelated investigation into Zacarias Moussaoui, who was taking flight lessons that the Minneapolis office suspected might be part of a plan to hijack a plane. However, having taken no action on the Phoenix memo, FBI headquarters was not sensitized to the potential threat and instructed Minneapolis that it could not share its complete Moussaoui report with the FAA.

These failures to "connect the dots" have become famous in the years since 9/11. However, that phrase oversimplifies a fundamental problem, not only with the sharing of information, but also with the way in which departments and agencies worked together.

II. Where We Are Now: *Evidence that Washington Can Work*

Over the last decade, our government has embarked on a "virtual reorganization" in how it answers the threat of terrorism. This shift in thinking has inspired reform in the way agencies and people collaborate and communicate. Top al-Qaeda leaders have been killed and new attacks on the homeland have been prevented because of this transformation in how agencies across government work together and share information in order to detect and preempt terrorist attacks. Substantial progress has been made in shifting the "need-to-know" culture toward a "need-to-share" paradigm, in which information flows more freely enabling greater collaboration between federal, state, and local agencies as well as the private sector.

Information is also increasingly decentralized and distributed. Informal and flexible groups of analysts from different parts of government and the private sector are able to work together and share expertise. Today, our government is able to function in hubs and spokes and distributed networks, empowering people at the edges of agencies instead of working in hierarchical pyramids. Information is shared, and teams from disparate parts of government go in and out of the National Counterterrorism Center and fusion centers nationwide. Ad hoc pursuit teams of experts or concerned officials form and disband as they see problems needing attention. The adoption of powerful social networking tools allows analysts to connect with colleagues throughout government. No longer must all information or requests for authority go up a chain of command or come down from on high.

We are pleased that the Markle Task Force contributed to this change by making recommendations that have been adopted in legislation, executive orders, and the 9/11 Commission Report. This Committee deserves special recognition for making these issues a priority and conducting continued oversight to measure progress. Both the Obama Administration and the Bush Administration have worked hard to put policies and processes in place to achieve these changes.

We are delighted that Ambassador McNamara is testifying today, as he played a critical role as the Program Manager for the Information Sharing Environment in making many of these changes.

The result of these reforms is that people within government are starting to work across agency lines in new and more powerful ways to understand the meaning of fragments of information and use that analysis to make better decisions. This "virtual reorganization" can be illustrated through three successes that were only possible because people worked together and shared information in ways that would have been considered impossible before 9/11.

1) Osama bin Laden was killed on May 2, 2011 as a result of a long-term, dedicated multi-agency mission that 9/11 Commission Chairman Lee Hamilton said unquestionably "came about as a result of reforms that . . . yielded much closer collaboration and intelligence sharing."[6] This story

[6] *Threats to the American Homeland After Killing Bin Laden: An Assessment: Hearing Before the H. Comm. On Homeland Sec.*, 112th Cong. (2011) (statement of Lee Hamilton).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01125 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.743

can be seen from press reports. Apparently, CIA led the effort that found al-Qaeda's leader, and the Joint Special Operations command, the National Security Agency ("NSA"), the National Geospatial-Intelligence Agency ("NGA"), and the Director of National Intelligence ("DNI") all played critical roles. These agencies are reported to have worked together seamlessly to provide the assault team as much information as possible on what they could expect to find at the compound. Teams of analysts sorted battlefield and all-source intelligence, designated subjects for additional collection, and conducted pattern analysis of relationships among terrorists, couriers, and raw data collected in the field. Collaboration between these agencies and departments helped weave together intelligence from a wide variety of sources in order to locate Bin Laden. Once the compound was identified, an interagency team, led by the CIA, reportedly developed and executed the raid brilliantly. The success of the Bin Laden mission built on the experience and trust gained from the interagency teams that fused intelligence operations and analysis in Iraq.

2) Najibullah Zazi was arrested in September 2009 in connection with an al Qaeda plot to bomb the New York City subway system. Again, press reports attribute this success to collaborative efforts, in this case those of the FBI, the Department of Homeland Security ("DHS"), and the New York and Denver police. Former DNI Dennis Blair also cited the Zazi case as "a prime example [of] the new level of cooperation among FBI, local law enforcement and U.S. intelligence agencies."[7] These agencies successfully thwarted one of the most serious terrorist threats since 9/11 by sharing information in ways that rarely occurred before the creation of state and local fusion centers and the FBI's Joint Terrorism Task Forces ("JTTFs"). According to press reports, counterterrorism analysts first became aware of a link between the Afghan-born Zazi and terrorists late in the summer of 2008, when he flew to Peshawar, Pakistan, a notorious terrorist haven. In September 2009, Zazi traveled to New York, where FBI agents and police detectives on the New York JTTF worked together to covertly monitor Zazi's activities. Press reports indicate that they used wiretaps, surveillance, and a secret court-ordered search to track Zazi and several of his associates. The Colorado Information Analysis Center ("CIAC"), a local fusion center created in response to 9/11, apparently provided analytic support to the Denver FBI and DHS after suspicious activity was reported to the CIAC through its website and 1-800 number.[8] In mid-September, the FBI arrested Zazi after he allegedly tried to build bombs with large quantities of hydrogen peroxide purchased at beauty shops in the Denver area. It is reported that Zazi, a U.S. citizen, had been trained in weapons and explosives in Pakistan and had made nine pages of handwritten notes on how to make and handle bombs. On February 22, 2010, Zazi pled guilty to terrorism charges. Although there were reportedly some internal disputes regarding the timing of Zazi's arrest, his movements were carefully monitored by several agencies, culminating in his arrest and conviction. John Brennan has praised Zazi's arrest as "represent[ing] the coordinated work of countless intelligence, homeland security and law enforcement personnel who have saved countless American lives."[9]

3) On May 1, 2010, because of improved watchlisting procedures, Faisal Shahzad was successfully apprehended after his attempt to detonate a car bomb in New York's Times Square. On May 3 — 53 hours and 20 minutes after he left Broadway — federal agents pulled him off of a Dubai-bound flight at JFK Airport, capturing him minutes before he could flee the country. This success was the direct result of improved use of the No Fly List. Although the watchlisting process is not perfect, the time line of events provided by the Terrorist Screening Center demonstrates how improved government watchlists can facilitate the rapid spread of critical information to intelligence and law enforcement agencies as well as private entities. After identifying Shahzad as

---

[7] Dennis C. Blair, Op-Ed, *Strengthening Our Nation's Front Line of Defense*, Wash. Post, Dec. 18, 2009.

[8] Department of Homeland Security, Fusion Center Success Stories: Fusion Center Supports Zazi Investigation, http://www.dhs.gov/files/programs/gc_1296488620700.shtm#8.

[9] John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at CSIS: Securing the Homeland by Renewing American Strength, Resilience and Values (May 26, 2010).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01126 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.744

the primary suspect in the attempted bombing, the FBI requested that Shahzad be nominated to the No Fly List at 11:40 a.m. on May 3. Within 24 minutes of this request he had been nominated to the No Fly List, and within 45 minutes the Transportation Security Administration was informed of his updated No Fly status. After another 47 minutes, all relevant federal agencies and all airlines were notified of the expedited update to the No Fly List. At 6:27 p.m., Shahzad made a phone reservation. Between 10:30 and 11:00 p.m., Customs and Border Patrol conducted a review of the final flight manifest for Shahzad's flight and identified Shahzad (the airline had run its last check against a list from the morning). At 11:02 p.m., Shahzad was removed from the flight and subsequently arrested. Although coordination between the government and the airlines was not perfect, the watchlist was still an effective information sharing tool because redundant checks were in place to ensure that the plane was not able to take off.

III. Where We Fall Short: *The Task Remains Enormous*

Now is not the time to declare victory. Today, our nation faces diverse threats. While the post-9/11 virtual reorganization has transformed our government and prepared us to face yesterday's terrorist threat, the recent arrest of Rezwan Ferdaus for plotting to attack the Pentagon with explosive-laden model airplanes and the tragedy this summer in Norway demonstrate that the threats we face have also transformed. Although al-Qaeda has been weakened by U.S. efforts overseas, the threats we face have become harder to detect. They are also closer to home because our enemy is more loosely coordinated and is less dependent on training camps in Afghanistan and Pakistan. For example, al-Qaeda offshoots have taken advantage of the Internet in an attempt to radicalize "lone wolves" in the U.S., including, according to press reports, well educated U.S. citizens such as Rezwan Ferdaus.

Much of the Intelligence Community and many in other agencies charged with national security have embraced the objective of collaborating across agency lines and sharing more information with those who need it to fulfill their mission. However, the February 2011 Government Accountability Office ("GAO") report on "high risk" government programs noted, "The government has continued to make progress during the past two years in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning Information Sharing Environment in place."[10] Implementation of information sharing programs has been uneven across agencies and has not been driven by a government-wide vision of the authorities and constraints necessary to build an effective and trusted information sharing environment.

An essential element of an information sharing environment is that prior to making information available to a wide community, the government should have regulations and processes for controlling access to and use of shared information.

Our ability to thwart the next Times Square bomber or another attack like Christmas Day, 2009 still depends too much on luck. Although substantial progress has been made over the past ten years, much still remains to be done, as reflected in recent reports by the GAO and the Congressional Research Service, which cite continued bureaucratic resistance in some agencies and call for developing a vision and roadmap for the future of information sharing.[11]

The government has successfully increased the free flow of information, but, as WikiLeaks' disclosure of hundreds of thousands of the State Department's diplomatic cables demonstrates, that increased information sharing has not always been implemented responsibly. Appropriate policies and technologies to limit the risk of unauthorized disclosure of sensitive information should have been in

[10] GAO, "High Risk Series: An Update," (Feb. 2011), p. 96, available at http://www.gao.gov/new.items/d11278.pdf (last visited 1 March 2011).

[11] GAO, "Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investment," (July 2011), available at http://www.gao.gov/products/GAO-11-455 (last visited 7 Oct. 2011); Congressional Research Service, "Intelligence Issues for Congress," (Sep. 21, 2011), available at http://www.fas.org/sgp/crs/intel/RL33539.pdf

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01127 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.745

place prior to making the leaked information accessible to a wide community, as described in detail below.

Addressing these challenges requires the focus to be on people and policies that build trust, not just technical standards for how to exchange more information. Progress in counterterrorism must continue to ensure that information can be located by analysts who need it, regardless of which agency has it.

IV. Where We Should be Going: *Recommendations and Next Steps*

Information sharing is a means, not an end. The ultimate goal is to change dramatically the way people in government work together across agencies by using technology and the best management know-how to direct human attention to the most pressing issues to facilitate collaboration and improve our ability to develop and act on intelligence. It is critical that in so doing, we protect traditional civil liberties. Done correctly, this can help address the problem of information overload and prevent future leaks while ensuring that decision-makers have timely access to the information they need to make better informed choices.

Four steps are critical to achieving this goal.

1. Strong leadership from the highest levels of government is required to sustain the progress made since 9/11 and drive our government to continue evolving to confront emerging 21st century challenges. The "virtual reorganization" on which our government embarked after 9/11 faces constant resistance. There is risk that it will be eroded as a result of bureaucratic turf battles and fears about information security. The leadership in Congress and the executive branch should persistently emphasize that the failure to share information is at least as dangerous as the risk that greater sharing might lead to disclosure of sensitive data. This Committee in particular has a critical oversight role to play. Continuing to hold hearings like this, supporting change, passing needed legislation — and providing adequate funds — are essential to ensure that these issues remain a top priority and that progress continues.

2. People with a valid mission must be able to discover that relevant information exists and access it under an authorized use standard.

An effective system for information sharing will make it possible for relevant data to be discovered in an automated manner, allowing both users and the data itself to find relevant information. This enables "data to find data," like an automated triage that helps direct human attention to the most pressing issues. When data finds data, people are no longer required to dream up every smart question because "relevance finds the user" – for example, through automatic alerts. To achieve this, data should be tagged with standardized information that can be indexed and searched.

A concept of authorized use also should be adopted. It provides a standard to determine whether a user is authorized to see what he or she has discovered. Like a library card catalogue that offers information on books, but not the books themselves, discoverability offers users the ability to discover select values (*e.g.*, who, what, where, when) without gaining access to the underlying data until they are granted permission based on a predicated purpose under the authorized use standard. This authorized use standard would overcome obstacles in the present system of classification by permitting an agency or its employees to obtain information based on their role, mission, and a predicated purpose.

An important Intelligence Community Directive, ICD 501, was issued in 2009 that represents a substantial step toward discoverability and authorized use. ICD 501 requires IC agencies to make all information collected and all analysis produced available for discovery by automated means. It also creates a "responsibility to provide." It includes elements of the authorized use standard as well. ICD 501 is being implemented throughout the Intelligence Community, but progress has been slow and much of the early implementation has focused on discovery of published reports. The implementation of ICD 501 should be accelerated and future efforts should extend to discovery of the underlying data, which is provided for under the Directive's existing language. The policies in ICD 501 should also be expanded to apply to relevant agencies outside the IC.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01128 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.746

Development of tools like discoverability and authorized use can help solve the current problem of information overload. In the case of the "Underwear Bomber's" nearly successful Christmas Day attack on Flight 253, the key information was available to a number of agencies, but was buried among hundreds of seemingly more dangerous leads. Markle's concept of "data finding data" could have helped make a connection that might have raised this threat out of the "background noise." For instance, when the embassy report from Umar Farouk Abdulmutallab's father was entered into the centralized TIDE database on terrorist identities, this new information should have been automatically linked to the fact that Abdulmutallab had been approved for a visa. An automatic e-mail alert could have brought this connection to the attention of the State Department adjudicator who granted that visa, which would likely have been revoked.

3. As new and more powerful ways of sharing information are developed, both privacy and security protections must be increased simultaneously in order to keep pace.

WikiLeaks is not an argument for less information sharing. Doing that would compromise our national security. The lesson from incidents like the WikiLeaks breach is that as we improve our capabilities to better share information, we should simultaneously deploy better policies and technologies to control its access and use. Security mechanisms, such as active audits that monitor behavioral changes and immutable audit logs, should be implemented along with dynamic permissioning and granular access controls, like the authorized use standard discussed above.

We should also increase privacy and civil liberties protections. While the development of robust privacy offices within key agencies like the DNI and the Department of Homeland Security represents significant progress, critical oversight mechanisms must also be established and supported. More detailed government-wide privacy policies that address the hard questions are necessary as well, as opposed to existing policies that state that agencies must comply with the law without providing guidance on how to do so.

These policies should address the new challenges posed by the evolving terrorist threat, such as al-Qaeda's increased use of U.S. citizens like Rezwan Ferdaus, who planned to use model aircraft filled with C-4 to attack targets in D.C., or Faisal Shahzad, the Times Square car bomber who was reportedly in contact with Anwar al-Awlaki, the radical U.S. citizen cleric in Yemen who was recently killed in a drone strike. Such policies must clearly address treatment of U.S. Person information, other persistent questions about secondary use and redress, and the emerging questions posed by the collection of vast amounts of data in the private sector. The government should also find ways to publicly discuss the legal authorities associated with data collection, sharing, and use as well in order to ensure public trust in the policies and adequate oversight.

Increasing both privacy and security protections will help build trust on two fronts. First, such protections will help the American people trust that the government is protecting their civil liberties. Second, they will help people within government trust each other when information is shared, confident that such activities are both secure and legal. Such a system of checks and balances builds trust that information is used in accordance with our nation's core values, enables greater public-private cooperation, and pushes decision making and initiative to the edges of the system — to local police, for example — where threats are most likely to be seen.

4. Information sharing is a tool that can help make the entire government more efficient. The issues associated with the trusted use of information in government decision-making are not unique to counterterrorism. Information sharing best practices can help decision-makers in all areas of government by giving them timely access to better information so they can make more informed choices.

Changing how people work together and use technology can make the whole of government more effective, as it has for many private sector businesses. In light of the very real fiscal constraints that our government faces today, we need to do more with less in many areas of national security including cybersecurity, counter proliferation, chemical and biological threats, and energy security. The answer is

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01129 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.747

not spending more money to create new institutions, like the host of fusion centers created after 9/11.

Instead, the focus should be on changing the culture within agencies through new business processes and technologies that empower trust and collaboration. Informal and flexible groups from different parts of government and the private sector should be able to work together on the full range of crosscutting issues to share expertise — as they do for counterterrorism. This flexible new way of working can empower people at the edges of agencies because information and requests for authorization no longer need to work their way up the chain of command as they do in government's traditional hierarchy.

The "virtual reorganization" that started after 9/11 has not been easy, but it demonstrates how much more effective our government can be when new ways of doing business allow people to collaborate horizontally across agencies and use information in new and more powerful ways. This transformation we are seeing in counterterrorism is built upon principles and practices that can be extended to other key homeland security priorities so that our government can work in a more modern, decentralized, public-private manner to address growing challenges like cybersecurity and economic security. The Obama Administration has already undertaken efforts to identify crosscutting areas in the President's budget where new management constructs can help leverage existing resources. Congress should work with the Administration through the budget process to increase efficiency by increasing the flow of information and empowering people who are closest to the facts on the ground to quickly form teams that draw on experts with different backgrounds in government, academia, and the private sector. This will provide decision-makers access to better information so they can make more informed choices, and this more agile decision making will save money.

***

We thank Chairman Lieberman, Senator Collins and the Committee for your leadership on these important issues.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01130 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.748

United States Government Accountability Office

GAO

Statement for the Record To the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, October 12, 2011

INFORMATION SHARING

Progress Made and Challenges Remaining in Sharing Terrorism-Related Information

Statement of Eileen R. Larence
Director, Homeland Security and Justice Issues

U.S. Government Accountability Office
GAO 90 YEARS 1921-2011
ACCOUNTABILITY * INTEGRITY * RELIABILITY

GAO-12-144T

67123.759

GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-144T, a statement for the record to the Committee on Homeland Security and Governmental Affairs, U.S. Senate

October 12, 2011

INFORMATION SHARING

Progress Made and Challenges Remaining in Sharing Terrorism-Related Information

Why GAO Did This Study

A breakdown in information sharing was a major factor contributing to the failure to prevent the September 11, 2001, terrorist attacks. Since then, federal, state, and local governments have taken steps to improve sharing. This statement focuses on government efforts to (1) establish the Information Sharing Environment (ISE), a government-wide approach that facilitates the sharing of terrorism-related information; (2) support fusion centers, where states collaborate with federal agencies to improve sharing; (3) provide other support to state and local agencies to enhance sharing; and (4) strengthen use of the terrorist watchlist. GAO's comments are based on products issued from September 2010 through July 2011 and selected updates in September 2011. For the updates, GAO reviewed reports on the status of Department of Homeland Security (DHS) efforts to support fusion centers, and interviewed DHS officials regarding these efforts. This statement also includes preliminary observations based on GAO's ongoing watchlist work. For this work, GAO is analyzing the guidance used by agencies to nominate individuals to the watchlist and agency procedures for screening individuals against the list, and is interviewing relevant officials from law enforcement and intelligence agencies, among other things.

What GAO Recommends

GAO is not making new recommendations, but has made recommendations in prior reports to federal agencies to enhance information sharing. The agencies generally agreed and are making progress, but full implementation of these recommendations is needed.

View GAO-12-144T. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

What GAO Found

The government continues to make progress in sharing terrorism-related information among its many security partners, but does not yet have a fully-functioning ISE in place. In prior reports, GAO recommended that agencies take steps to develop an overall plan or roadmap to guide ISE implementation and establish measures to help gauge progress. These measures would help determine what information sharing capabilities have been accomplished and are left to develop, as well as what difference these capabilities have made to improve sharing and homeland security. Accomplishing these steps, as well as ensuring agencies have the necessary resources and leadership commitment, should help strengthen sharing and address issues GAO has identified that make information sharing a high-risk area.

Federal agencies are helping fusion centers build analytical and operational capabilities, but have more work to complete to help these centers sustain their operations and measure their homeland security value. For example, DHS has provided resources, including personnel and grant funding, to develop a national network of centers. However, centers are concerned about their ability to sustain and expand their operations over the long term, negatively impacting their ability to function as part of the network. Federal agencies have provided guidance to centers and plan to conduct annual assessments of centers' capabilities and develop performance metrics by January 2012 to determine centers' value to the ISE. DHS and the Department of Justice are providing technical assistance and training to help centers develop privacy and civil liberties policies and protections, but continuous assessment and monitoring policy implementation will be important to help ensure the policies provide effective protections.

In response to its mission to share information with state and local partners, DHS's Office of Intelligence and Analysis (I&A) has taken steps to identify these partner's information needs, develop related intelligence products, and obtain more feedback on its products. I&A also provides a number of services to its state and local partners that were generally well received by the state and local officials we contacted. However, I&A has not yet defined how it plans to meet its state and local mission by identifying and documenting the specific programs and activities that are most important for executing this mission. The office also has not developed performance measures that would allow I&A to demonstrate the expected outcomes and effectiveness of state and local programs and activities. In December 2010, GAO recommended that I&A address these issues, which could help it make resource decisions and provide accountability over its efforts.

GAO's preliminary observations indicate that federal agencies have made progress in implementing corrective actions to address problems in the watchlisting process that were exposed by the December 25, 2009, attempted airline bombing. These actions are intended to address problems in the way agencies share and use information to nominate individuals to the watchlist, and use the list to prevent persons of concern from obtaining visas and boarding planes to the United States, among other things. These actions can also have impacts on agency resources and the public, such as traveler delays and other inconvenience. GAO plans to report the results of this work later this year.

United States Government Accountability Office

Chairman Lieberman, Ranking Member Collins, and Members of the Committee:

I am pleased to submit this statement on the progress federal agencies have made and the challenges they face in sharing and managing terrorism-related information.[1] The nation just passed the 10-year anniversary of the September 11, 2001, terrorist attacks. The 9/11 Commission concluded that a breakdown in information sharing was a major factor contributing to the failure to prevent those attacks. Since then, enactment of the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act) and other legislation called for substantial changes in the way agencies share information on terrorist threats.[2] In addition, federal, state, and local governments have taken steps to improve information sharing. However, in part based on the December 25, 2009, attempted airline bombing, questions have been raised about how well the government is using and sharing terrorism-related information to identify potential threats that individuals may pose. These acts of terrorism on U.S. soil underscore the importance of the federal government's continued need to ensure that terrorism-related information is shared with stakeholders across all levels of government, the private sector, and foreign countries in an effective and timely manner.

Since January 2005, we have designated terrorism-related information sharing as high risk because the government continues to face serious challenges in analyzing key information and sharing it among federal, state, local, and other security partners in a timely, accurate, and useful way. We have since monitored federal efforts to implement the Information Sharing Environment (ISE)—a government-wide approach that facilitates the sharing of terrorism-related information, which may

[1] Terrorism-related information includes homeland security, terrorism, and weapons of mass destruction information. See 6 U.S.C. §§ 482(f)(1), 485(a)(1), (5)-(6).

[2] See, e.g., Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664-70 (codified as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 504, 121 Stat. 266, 313-17, at 6 U.S.C. § 485).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01133 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.761

include any method deemed necessary and appropriate.[3] This area remained high risk in our February 2011 update.[4]

A major focus of the ISE has been to improve the sharing of terrorism-related information between the federal government and state and local security partners. After the terrorist attacks of September 11, 2001, state and local governments began to establish fusion centers to address gaps in terrorism-related information sharing that the federal government cannot address alone and provide a mechanism for information sharing within the state. Pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), the Department of Homeland Security (DHS) created the State, Local, and Regional Fusion Center Initiative to establish partnerships with state, local, and regional fusion centers.[5] In coordination with fusion centers and the states, DHS is to take steps to support efforts to integrate the centers into the ISE, assign personnel to centers, and provide training and funding, among other things. In recent years, fusion centers have been credited with being influential in disrupting a planned terrorist attack on the New York City subway system, investigating bomb threats against U.S. airlines, and providing intelligence support to several political conventions and summits. Today, there are 72 fusion centers nationwide.[6]

In addition to supporting fusion centers, DHS has responsibility for, among other things, sharing terrorism-related information with its state and local partners, as appropriate. DHS's Office of Intelligence and Analysis (I&A) is the lead DHS component with responsibilities for

[3] See 6 U.S.C. § 485(a)(3).

[4] GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 16, 2011).

[5] See Pub. L. No. 110-53, § 511, 121 Stat. at 317-24 (codified at 6 U.S.C. § 124h).

[6] All 50 states have designated a primary fusion center to serve as the focal point for information sharing. According to the Office of the Program Manager for the ISE, 1 of the 50 states has not yet established the capabilities to be recognized by the federal government. In general, these fusion centers are statewide in jurisdiction and are operated by state entities, such as the state police or bureau of investigation. In addition, 22 major urban areas have established their own fusion centers, which are regional centers that usually cover large cities with substantial populations and numerous critical infrastructure sites and may be operated by city or county law enforcement or emergency management agencies. For purposes of this report, "fusion centers" is used to refer to both state and major urban area fusion centers.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01134 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.762

meeting this mission. We have assessed, at the Congress' request, how well the office has been able to meet this mission and give priority to state and local sharing from among I&A's other competing functions. The results of this work are discussed later in this statement.

Another way the government uses information sharing as a counterterrorism tool is through the terrorist watchlist process. The attempt on December 25, 2009, to detonate a concealed explosive onboard a U.S.-bound aircraft raised questions as to why warnings about the attempted bomber did not result in the U.S. government including him in its consolidated terrorist database. The Terrorist Screening Center—administered by the Federal Bureau of Investigation—is responsible for maintaining this list of known or suspected terrorists and making information from the Terrorist Screening Database (TSDB) available, as appropriate, to agencies that screen individuals for possible threats. For instance, subsets of the TSDB are used by DHS's Transportation Security Administration (TSA) to screen individuals before they board an aircraft and by U.S. Customs and Border Protection to screen travelers entering the United States.

My statement discusses the results of our work in monitoring four important information sharing issues: (1) progress made and work remaining in establishing the ISE; (2) federal agencies' efforts to help fusion centers build capabilities; (3) how DHS has responded to its statutory mission to share terrorism-related information with state and local partners; and (4) government actions to improve the watchlist process as a result of the December 2009 attempted airline bombing.

This statement is based on products we issued from September 2010 through July 2011 and selected updates in September 2011.[7] In conducting our prior work, we analyzed documents, including key statutes, agency policies, and best practices. We also interviewed officials at the various federal, state, and local entities with responsibilities for

[7] This statement is primarily based on our most recent reports on the ISE, fusion centers, and I&A. See, GAO, *Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments*, GAO-11-455 (Washington, D.C.: July 21, 2011); *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could Better Measure Results*, GAO-10-972 (Washington, D.C.: Sept. 29, 2010); and *Information Sharing: DHS Could Better Define How It Plans to Meet Its State and Local Mission and Improve Performance Accountability*, GAO-11-223 (Washington, D.C.: Dec. 16, 2010).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01135 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.763

information sharing initiatives that are discussed in this statement. Our previously published reports contain additional details on the scope and methodology for those reviews. For the updates, we reviewed documentation on the status of DHS's efforts to support fusion centers and interviewed DHS officials regarding these efforts. This statement is also based on our ongoing work on the terrorist watchlist that we are conducting for this Committee, the House Committee on Homeland Security, and the House Committee on Oversight and Government Reform. For this ongoing work, we are analyzing the guidance used by agencies to nominate individuals to the watchlist and agency procedures for screening individuals against the list, and interviewing relevant officials from law enforcement and intelligence agencies, among other things. We conducted all of our work in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Agencies Have Improved Sharing as They Build the ISE, but a Better Roadmap and System of Accountability Could Guide Future Development

ISE Has Improved Sharing By Advancing Goals and Priority Programs

In our July 2011 report, we noted that the Program Manager for the ISE and key security agencies have continued to make progress in addressing issues that keep terrorism-related information sharing on our high-risk list.[8] For example, they developed a corrective action plan—or framework—to implement a set of initial goals and priority programs that

[8] GAO-11-455.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01136 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.764

help to establish the ISE, partly responding to recommendations we made in 2008.[9] Goals included reducing barriers to sharing and improving information sharing practices with federal, state, local, tribal, and foreign partners. Priority programs included developing common information sharing standards; building a national integrated network of fusion centers; implementing a system whereby state and local partners can report suspicious activity; and controlling and handling sensitive but unclassified information. Activities under the framework also included establishing information sharing incentive programs for federal employees and strengthening privacy, civil rights, and civil liberties considerations. The administration has recognized, however, that the framework was useful in promoting this initial set of programs and activities, but it did not define what the fully functioning ISE is to achieve and include. Therefore, as discussed in the following sections, the framework does not provide the comprehensive roadmap that is needed to further develop and implement the ISE going forward.

More Fully Defining the ISE, Related Costs, and What Work Remains Would Help Provide a Roadmap and Accountability for Results

Defining an End State Vision

The Program Manager has acknowledged the importance of defining what the ISE is intended to achieve and include—or the "end state" vision—and noted that he is doing so as part of ongoing efforts to update the 2007 National Strategy for Information Sharing. He said that this update will drive future ISE implementation efforts and will help individual agencies adapt their information sharing policies, related business processes, architectures, standards, and systems to effectively operate within the ISE. The Program Manager also noted that after development of the end state vision is completed, supporting implementation plans will be needed to help guide achievement of the vision, including plans that define what activities and initiatives will be needed to achieve the end

[9] See GAO, *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492 (Washington, D.C.: June 25, 2008).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01137 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.765

state and guide ISE development and implementation. Such plans would be consistent with our recommendation for a roadmap if they contain key elements such as roles, responsibilities, and time frames for these activities, among other things.

Leveraging Agency Initiatives

Consistent with the Intelligence Reform Act, the ISE is to provide the means for sharing terrorism-related information across five communities—homeland security, law enforcement, defense, foreign affairs, and intelligence—in a manner that, among other things, leverages ongoing efforts. As we reported in July 2011, the ISE has primarily focused on the homeland security and law enforcement communities and related sharing between the federal government and state and local partners, in part to align with information sharing priorities outlined by the administration. We recognize that recent homeland security incidents and the changing nature of domestic threats make continued progress in improving sharing between federal, state, and local partners critical. However, consistent with the Intelligence Reform Act, the ISE is intended to provide the means for sharing terrorism-related information across all five communities.

The Program Manager and ISE agencies have not yet ensured that initiatives within the foreign affairs, defense, and intelligence communities have been fully leveraged by the ISE to enhance information sharing within and across all communities. For example, according to Department of State (State) officials, the department shares terrorism-related information with other agencies through a variety of efforts and initiatives related to national and homeland security, but State initiated these efforts independently and not through the Office of the Program Manager. According to the Program Manager, State also possesses information about entrants to the country that could be valuable to the ISE. However, in April 2011, State officials said that the Office of the Program Manager had not contacted the department's coordinator for the ISE to request information on programs or initiatives related to people entering the country to determine if this information could be useful to the broader ISE communities. Further, intelligence agencies have technology initiatives—including new ways of ensuring that authorized users have access to, and are able to search across, classified systems and networks to facilitate information sharing—but it is not clear to what extent transferring this best practice to non-classified information is being considered under the ISE.

The Program Manager also noted that his office has engaged all five communities in ISE activities. For example, in addition to working with the homeland security and law enforcement communities, he said his office

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01138 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.766

has worked with State to standardize terrorism-related information sharing agreements with foreign governments; with the Department of Defense to develop information technology standards that allow different agencies to exchange information; and the intelligence community to develop terrorism-related information products for state, local, and tribal governments. He also noted that all five communities have been afforded opportunities to help set ISE programmatic priorities. However, the Program Manager and agencies had not yet taken actions to ensure that all relevant information sharing initiatives across the five communities are fully leveraged, which could help enhance information sharing government-wide. In our July 2011 report, we recommended that they take such actions. They generally agreed and have started to address this issue.

Defining Incremental Costs

The Program Manager and agencies have not yet identified the incremental costs necessary to implement the ISE, as envisioned by the Intelligence Reform Act. Our prior work shows that cost information can help agencies allocate resources and investments according to priorities and constraints, track costs and performance, and shift such investments and resources as appropriate.[10] We recognize that developing accurate and reliable incremental cost estimates for the ISE is a difficult undertaking, complicated further by the fact that the Program Manager and agencies are still defining what the ISE is, is to include, and is to attain. In our July 2011 report, we recommended that the Program Manager—in coordination with the Office of Management and Budget—task the key ISE agencies to define, to the extent possible, the incremental costs needed to help ensure successful implementation of the ISE. The Deputy Program Manager acknowledged the importance of identifying incremental costs and noted that the Office of the Program Manager will continue to work directly with the Office of Management and Budget to provide agencies with budget guidance that calls for them to identify their costs to implement the ISE.

Demonstrating Progress

The Intelligence Reform Act requires the Program Manager to, among other things, monitor implementation of the ISE by federal departments and agencies to ensure adequate progress is being made and regularly report the findings to Congress. In June 2008, we reported that the Office of the Program Manager was monitoring ISE implementation—as

[10] See GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, GAO-04-408T (Washington, D.C.: Feb. 3, 2004).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01139 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.767

demonstrated through its annual report to Congress—but that such monitoring did not include an overall assessment of progress in implementing the ISE and how much work remained. Thus, we recommended, among other things, that the Program Manager develop a way to measure and demonstrate results and to show the extent to which the ISE had been implemented, as well as more fully define the key milestones needed to achieve the ISE.[11] The Program Manager generally agreed and in January 2011, the Information Sharing and Access Interagency Policy Committee (ISA IPC) and the Office of the Program Manager initiated an effort to make ISE priority programs and related goals more transparent and to better monitor progress.[12] Specifically, according to the Deputy Program Manager, agencies that are responsible for implementing ISE priority programs are leading efforts to establish 3-, 6-, and 12-month goals for these programs. Information on progress made in reaching these goals may be included in future ISE annual reports. In addition he explained that the Office of the Program Manager is working with agencies to develop a performance management framework that will be linked to the updated national strategy. These actions should help to provide an accurate accounting for progress to Congress and other stakeholders and would be consistent with the criteria we use to evaluate a program's risk, which calls for a way to demonstrate progress and results.

Governing the ISE

Our prior work on high-risk issues shows that a strong commitment from top leadership to address problems and barriers to sharing terrorism-related information is important to reducing related risks. In July 2009, the White House established the ISA IPC to subsume the role of its predecessor interagency body—the Information Sharing Council.[13] The Program Manager at that time cited concerns about the Program Manager's authority and provided recommendations intended to help

[11] GAO-08-492.

[12] Interagency Policy Committees—within the Executive Office of the President—are the main day-to-day fora for interagency coordination of national security policy, providing policy analysis and ensuring timely responses to decisions made by the President. See, Executive Office of the President, *Presidential Policy Directive-1: Organization of the National Security Council System* (Washington, D.C.: Feb. 13, 2009).

[13] The Information Sharing Council—composed of senior representatives from federal departments and agencies, some of who possess and acquire terrorism-related information—was established in accordance with the Intelligence Reform Act to assist the President and the Program Manager with their ISE responsibilities. See 6 U.S.C. § 485(g).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01140 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.768

strengthen the ISE effort.[14] For example, among other things, he recommended that the Program Manager be appointed by the President and serve as co-chair of the ISA IPC. Subsequently, both changes were implemented, which were intended to bring high-level policy decision making and oversight to the development of the ISE. At the time of our review, it was too early to tell how the new structure would impact the continued development and implementation of the ISE and if the Program Manager's new role would provide him sufficient leverage and authority to ensure that agencies fully participate in the ISE.

The Enterprise Architecture Management Foundation for Supporting ISE Implementation Could Be Improved

In our July 2011 report, we noted that the process of defining an enterprise architecture (EA) for the ISE could help the Program Manager and agencies in their efforts to define the current operational and technological capabilities within the ISE, the future capabilities needed, and a plan to transition between the two.[15] Under an EA approach, agencies are to define the business processes involved in information sharing, map out the exchange of information to be achieved, and build the technology and other resources they need to accomplish the sharing in their EA plans and budget requests, among other things. Doing so could help the government more fully define the necessary components of the ISE. We reported that agencies had begun to build ISE initiatives, such as suspicious activity reporting, into their EAs. To better define ISE EA guidance and effectively manage EA architecture, we recommended that the Program Manager, ISA IPC, and agencies establish an EA management plan for the ISE to improve ISE EA management practices and address missing architecture content and a mechanism to ensure implementation. The Program Manager and the Office of Management

[14] Beyond ISE Implementation: Exploring the Way Forward for Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security, 111th Cong. 5 (2009) (statement of Ambassador Thomas E. McNamara, Program Manager, Information Sharing Environment, Office of the Director of National Intelligence).

[15] An EA can be viewed as a reference or "blueprint" for achieving strategic business goals and outcomes, including maximizing information sharing within and across organization boundaries. A well-defined EA provides a clear and comprehensive picture of an entity, whether it is an organization (e.g., federal department or agency) or a functional or mission area that cuts across more than one organization (e.g., homeland security) by documenting the entity's current operational and technological environment and its target environment, as well as a plan for transitioning from the current to the target environment.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01141 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.769

and Budget generally agreed and are taking steps to address the intent of this recommendation.

Federal Agencies Are Helping Fusion Centers Build Capabilities, but Have More Work to Help Them Sustain Operations and Measure Their Value

Federal Agencies Have Provided Resources to Develop a National Fusion Center Network, but Centers Are Concerned about Sustaining Operations

The federal government recognizes that fusion centers represent a critical source of local information about potential threats, including homegrown terrorism, and a means to disseminate terrorism-related information and intelligence from federal sources. DHS, which has a statutory lead for state and local information sharing, in collaboration with the Department of Justice (DOJ) and the Program Manager for the ISE, has taken steps to partner with and leverage fusion centers—a top priority for the ISE. In accordance with the 9/11 Commission Act, over the years, DHS has provided centers with a variety of support, including personnel assigned to centers, access to classified and unclassified homeland security and terrorism information and systems, training and technical assistance, and federal grant funding. For instance, as of July 2010, DHS had deployed 74 intelligence officers to fusion centers. In addition, states have reported to DHS that they have used about $426 million in grant funding from fiscal year 2004 through 2009 to support fusion-related activities nationwide.[16]

[16] The $426 million in grant funding was as of June 16, 2010, and included all Federal Emergency Management Agency (FEMA) preparedness grant programs. This funding was for activities aligned to project types that support fusion center activities, such as the following: establish/enhance a terrorism intelligence/early warning system, center, or task force; establish/enhance public-private emergency preparedness program; and develop/enhance homeland security/emergency management organization and structure. Funding data are self-reported by grantees and, according to FEMA officials, are not validated to ensure that funds were exclusively used to support fusion center activities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01142 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.770

In September 2010, we reported that fusion centers cited federal funding as critical to their long-term sustainability and to achieving and maintaining a set of baseline capabilities. These baseline capabilities were defined by the federal government and fusion centers as being necessary for centers to be considered capable of performing basic functions in the national information sharing network. They include, for example, capabilities related to information gathering, recognition of indicators and warnings, and intelligence and information dissemination. According to a survey of all fusion centers conducted by DHS and the Program Manager for the ISE, of the 52 fusion centers that responded, on average, over half of their 2010 budgets were supported by federal funding.[17]

Concerns about and challenges related to funding for sustainability are long-standing issues. Fusion centers do not have their own federal funding source but must compete each year with other state homeland security, law enforcement, and emergency management agencies and missions for a portion of the total federal homeland security grant funding awarded to each state. We and others have reported on the centers' concerns about the lack of a predictable funding source. For example, in September 2010 we reported that officials in all 14 fusion centers we contacted stated that without sustained federal funding, centers could not expand operations to close the gaps between their current operations and the baseline capabilities, negatively impacting their ability to function as part of the national network.[18]

Senior DHS officials have acknowledged the fusion centers' concerns and in an effort to further prioritize the development of the national network of fusion centers, DHS revised fiscal year 2011 grant guidance. It now requires, among other enhancements, that (1) each state submit a fusion center investment justification and (2) the justification must be related to mitigating capability gaps.[19] Nevertheless, concerns about federal funding

[17] This figure is based on information reported to the Program Manager of the ISE by 52 of 72 fusion centers. Information was aggregated, but not verified, by the Program Manager or GAO.

[18] GAO-10-972.

[19] A fusion center typically contributes to the development of a state's federal grant application by providing information on how it will use the proposed funding needed, called an investment justification.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01143 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.771

could be exacerbated given that overall homeland security grant funding of $2.1 billion for fiscal year 2011 is $780 million less than the previous year.

Federal Agencies Plan to Assess Centers' Capabilities and Develop Performance Metrics to Determine Centers' Value to the ISE

Consistent with efforts to develop this national network of fusion centers, federal agencies have also issued a series of guidance documents, including the baseline capabilities, to support fusion centers in establishing their operations.[20] The baseline capabilities are intended to help ensure that a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information.

As a first step, the Program Manager for the ISE, DHS, and DOJ conducted a systematic assessment of centers' capabilities in 2010 and analyzed results to identify strengths, gaps, and weaknesses across the national network of fusion centers. The assessment specifically focused on four operational capabilities identified as critical which are generally defined as a fusion center's ability to receive, analyze, disseminate, and gather information.[21] The assessment also focused on centers' progress in implementing privacy, civil rights, and civil liberties protections. The results of this assessment and a subsequent survey effort conducted in January 2011 showed that over half of the 72 fusion centers had developed and implemented a final written plan, policy, or standard operating procedure to achieve three of the four capabilities—receive (44 centers), disseminate (46 centers), and gather (42 centers). However, 37 centers indicated that they had not implemented a plan related to developing capabilities to analyze time sensitive information.

[20] Global Justice Information Sharing Initiative, *Baseline Capabilities for State and Major Urban Area Fusion Centers, A Supplement to the Fusion Center Guidelines* (September 2008).

[21] According to DHS, personnel from DHS, the Program Manager for the ISE, and DOJ coordinated with state and local government representatives and fusion center officials to jointly identify these critical operational capabilities to be priontized in developing the national network of fusion centers. Specifically, the four operational capabilities are defined as: (1) receive: ability to receive classified and unclassified information from federal partners; (2) analyze: ability to assess local implications of threat information through the use of a formal risk assessment process; (3) disseminate: ability to further disseminate threat information to other state, local, tribal, territorial, and private sector entities within their jurisdiction; and (4) gather: ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01144 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.772

According to DHS officials who oversee the fusion center initiative, using the results of the 2010 assessment, along with feedback obtained from fusion center directors, DHS developed and implemented a Fusion Center Assessment Process in 2011. This process will be conducted annually to identify capability gaps, enable gap mitigation planning, and continue to drive the allocation of resources to mitigate those gaps. DHS expects to release the results of the 2011 assessment in January 2012, according to DHS officials.

We also reported in September 2010 that if centers are to receive continued federal financial support, it is important that they are also able to demonstrate their impact and value added to the national network and the nation's overall information sharing goals. However, the federal government had not established standard performance measures that it could use across all fusion centers to assess their contributions. We recommended that DHS define the steps it needed to take to design and implement a set of measures and commit to a target timeframe for their completion. According to senior DHS officials overseeing the office, in March 2011, the State and Local Program Office and a representative group of fusion center directors began developing an overarching strategy document to define the vision, mission, goals, objectives, and specific outcomes that fusion centers will be expected to achieve, and associated performance measures for the national network of fusion centers. According to these officials, such performance measures are to be in place by the end of 2011.

DHS and DOJ Are Helping Centers Develop Privacy and Civil Liberties Policies and Protections but Monitoring Implementation Will Be Important

Because fusion centers collect, analyze, and disseminate information on potential criminal and terrorist threats, some entities, such as the American Civil Liberties Union, have raised concerns that centers are susceptible to privacy and civil liberties violations. We reported in September 2010 that consistent with federal requirements, DHS and DOJ have provided technical assistance and training to help centers develop privacy and civil liberties policies and protections. For example, DHS and DOJ provided fusion centers with guidance and technical assistance, including a template on which to base a privacy policy and a process for reviewing centers' policies to ensure they are consistent with federal requirements. DHS reported that all operational fusion centers now have a final, approved privacy policy in place that is at least as comprehensive

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01145 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.773

as the ISE Privacy Guidelines.[22] With respect to training, we reported that DHS, in partnership with DOJ and other entities, has implemented a three-part training and technical assistance program in support of fusion centers' efforts to provide appropriate privacy, civil rights, and civil liberties training for personnel. We also reported that DHS, in conjunction with DOJ and the Program Manager for the ISE, was taking steps to assess the implementation of centers' privacy protections to ensure that the protections described in centers' policies were implemented in accordance with all applicable privacy regulations, laws, and constitutional protections. Federal agencies are also encouraging centers to assess their own protections to identify any existing privacy and civil liberties risks and to develop strategies to mitigate the risks. Continuous assessment and monitoring are key steps to help ensure that fusion centers are implementing privacy and civil liberties protections and that DHS, and other federal agencies, are supporting them in their efforts.

DHS Has Enhanced Support to State and Local Partners but Could Better Define the Actions It Will Take to Meet This Mission and Measure Progress

In addition to supporting fusion centers, DHS is responsible for sharing terrorism-related information with its state and local partners, and within DHS, I&A is the designated lead component for this mission. In December 2010, we reported that I&A had initiatives underway to identify state and local information needs, developing intelligence products to meet these needs, and obtaining more detailed feedback on the timeliness and usefulness of these products, among other things.[23] I&A also provided a number of services to its state and local partners—primarily through fusion centers—that were generally well received by the state and local officials we contacted. For example, in addition to deploying personnel and providing access to networks disseminating classified and unclassified information, I&A provides training directly to state and local personnel and operates a 24-hour service to respond to state and local requests for information and other support.

[22] In 2006, the Program Manager for the ISE issued the ISE Privacy Guidelines, which establish a framework for sharing information in the ISE in a manner that protects privacy and other legal rights. The ISE Privacy Guidelines apply to federal departments and agencies and, therefore, do not directly impose obligations on state and local government entities. However, the ISE Privacy Guidelines do require federal agencies and the Program Manager for the ISE to work with nonfederal entities, such as fusion centers, seeking to access protected information to ensure that the entities develop and implement appropriate policies and procedures that are at least as comprehensive as those contained in the ISE Privacy Guidelines.

[23] GAO-11-223.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01146 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.774

We also reported that a Congressional committee that had been trying to hold I&A accountable for achieving its state and local mission was concerned about I&A's inability to demonstrate the priority and level of investment it is giving to this mission compared to its other functions, as evidenced by hearings conducted over the past several years. We reported that, historically, I&A had focused its state and local efforts on addressing statutory requirements and responding to I&A leadership priorities. However, I&A had not yet defined how it plans to meet its state and local information-sharing mission by identifying and documenting the specific programs and activities that are most important for executing this mission. Our prior work has found that successful organizations clearly articulate the programs and activities that are needed to achieve specified missions or results, and the organization's priorities, among other things.[24]

Further, we reported that I&A had not defined what state and local information-sharing results it expected to achieve from its program investments and the measures it would use to track the progress it is making in achieving these results. For example, all of I&A's state and local measures provided descriptive information regarding activities and services that I&A provided, such as the percentage of fusion centers with I&A personnel and the number of requests for support. However, none of these measures accounted for the actual results, effects, or impacts of programs and activities or the overall progress I&A is making in meeting its partners' needs. For example, the personnel measure did not provide information related to the effectiveness of the I&A personnel or the value they provide to their customers, such as enhanced information sharing, analytic capabilities, and operational support.

To help I&A strengthen its efforts to share information with state and local partners, we recommended, among other things, that I&A (1) identify and document priority programs and activities related to its state and local mission, and (2) take actions to develop additional performance measures that gauge the results that I&A's information-sharing efforts have achieved and how they have enhanced homeland security. By taking these steps, I&A could potentially increase the usefulness of its products and services; the effectiveness of its investments; and the

[24] See, for example, GAO, *Results-Oriented Government: GPRA Has Established a Solid Foundation for Achieving Greater Results*, GAO-04-38 (Washington, D.C.: Mar. 10, 2004).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01147 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.7/5

organization's accountability to Congress, key stakeholders, and the public. DHS agreed with these recommendations and expects to address them as part of new strategic planning efforts.

Agencies Are Addressing Watchlisting Gaps but Could Benefit from Assessing Impacts of Changes

The Executive Office of the President's review of the December 2009 attempted airline bombing found that the U.S. government had sufficient information to have uncovered and potentially disrupted the attack, but shortcomings in the nominations process resulted in the failure to nominate the attempted bomber for inclusion in the TSDB.[25] Thus, screening agencies that could have identified him as a potential threat were unable to identify him and take action. The Executive Office of the President tasked departments and agencies to undertake a number of corrective actions to help address such gaps.[26] We have ongoing work to assess the changes implemented and their impacts. This work is assessing (1) the actions the federal government has taken since the attempted attack to strengthen the watchlist nominations process, as well as any resulting challenges and impacts; (2) how the composition of the TSDB changed as a result of agency actions; and (3) how screening agencies are addressing vulnerabilities exposed by the attempted attack, the outcomes of related screening, and the extent to which federal agencies assessing the impacts of this screening.

Our preliminary observations show that federal agencies have made progress in implementing corrective actions to address problems in the nominations process that were exposed by the December 2009 attempted attack. These actions are intended to address problems in the way agencies share and use information to nominate individuals to the TSDB, and use the watchlist to prevent persons of concern from boarding planes to the United States or entering the United States at a port of entry. For example, according to TSA, the agency's assumption of the screening function from air carriers—under the Secure Flight program—has improved the government's ability to correctly determine whether passengers are on the No Fly or Selectee lists and has resulted in more individuals on these lists being identified and denied boarding an aircraft

[25] Executive Office of the President, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, D.C.: Jan. 7, 2010).

[26] Executive Office of the President, *Memorandum on Attempted Terrorist Attack on December 25, 2009: Intelligence, Screening, and Watchlisting System Corrective Actions* (Washington, D.C.: Jan. 7, 2010).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01148 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.776

or subjected to additional physical screening before they board, as appropriate. Also, in April 2011, TSA began screening airline passengers against a broader set of TSDB information, which has helped mitigate risks. As part of its border and immigration security mission, CBP implemented the Pre-Departure Targeting Program to expand its practice of identifying high-risk and improperly documented passengers—including those in the TSDB—before they board flights bound for the United States, and recommending that air carriers deny boarding to individuals that the agency would likely deem inadmissible upon arrival at a U.S. airport. This program has resulted in more known or suspected terrorists being denied boarding.[27]

Our preliminary work also suggests that the outcomes of these DHS programs demonstrate the homeland security benefits of terrorist-related screening, but such screening could have impacts on agency resources and the traveling public. For example, new or expanded screening programs have could require agencies to dedicate more staff to check traveler information against watchlist information and take related law enforcement actions. Also, new or expanded screening programs could result in more individuals misidentified as being in the TSDB, which can cause traveler delays and other inconvenience. It will be important for agencies to monitor and address these impacts as appropriate moving forward. We plan to issue a report with the final results or our work later this year.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, this concludes my statement for the record.

Contacts and Acknowledgments

For additional information regarding this statement, please contact Eileen R. Larence at (202) 512-6510 or larencee@gao.gov. In addition, Eric Erdman, Mary Catherine Hult, Thomas Lombardi, Victoria Miller, and Hugh Paquette made key contributions to this statement. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

[27] Known or suspected terrorists that are U.S. citizens or lawful permanent residents generally may not be prevented from boarding flights bound for the United States.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01149 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.777

Post-Hearing Questions for the Record
Submitted to the Honorable John E. McLaughlin
From Senator Joseph I. Lieberman

"Ten Years After 9/11: A Status Report on Information Sharing"
October 12, 2011

1. **In your prepared testimony, you note that "there is not a common and widely-shared vision among national security specialists of the end state they want to achieve on information technology and information sharing."**

   Why do you believe that this common vision of an end state does not exist? What are the key impediments to achieving this? Who in the United States government do you believe has lead responsibility for establishing and implementing this vision?

There has been substantial progress on these issues since 9/11, but different agencies still tend to give priority to what they need from information technology to do their individual jobs as opposed to what is needed to collaborate effectively across agency lines. Many agencies have developed advanced and excellent systems for internal collaboration. But they typically do not have a common vision of what a community-based system would look like – that is, a system that would serve all of them equally and facilitate interagency work.

The key impediments to achieving a common end state are: Most agencies format and tag their data differently; there has not been a common standard across the community for identifying and certifying those seeking to access data (the virtual equivalent of now-achieved community badge); there are different standards for storage and retrieval of data; and different capacity needs and budgets.

To create a community system – one that allows all agencies to exchange data, collaborate on line, and search a wide array of community data bases (from different agencies) through a common access portal – decisions are required about what standards will be commonly adopted for things like data entry, storage, retrieval, and access for those seeking to acquire data. Any decisions will involve adjustments by all agencies by varying degree –

adjustments that will be costly both in personnel and budget terms and that some will object to as too costly or complicated.

Only the DNI can drive this process and make the necessary decisions. To his credit, DNI Clapper understands this and appears to be stepping up to the challenge. He has charged CIA and NSA in particular to lead a community-wide effort that, if I understand it correctly, will head in the direction I've outlined above. This is in the early stages and we will have to wait and see.

2. **In your testimony you noted "a subtle kind of risk aversion" within the US intelligence community in dealing with data that touches American citizens, and that in many cases, "intelligence agencies were not going to the limit of what the law allowed them."**

   What should be done to reduce such risk aversion – either at the organizational level or at the individual level – with respect to the use of such data?

In my study of this, undertaken for DNI Blair, I concluded that different agencies – and different officers within agencies – had varying interpretations of what the law permitted. There was a great deal of confusion on this score. The result is that leads can go unpursued or that legitimate intelligence may not be not acted upon.

The first task to correct this is largely educational. The general counsels of the agencies need to review with the affected officers how to interpret existing laws, seeking clarity and common understanding about what is permitted and what is not. At more senior levels, the DNI and appropriate elements of DoJ might caucus on this as well – in an effort to make sure the existing laws are understood, sufficient to the task, and observed correctly.

The problem is not that people are exceeding the law, pushing the boundaries, or infringing on peoples' privacy. It is quite the reverse -- more a matter of uncertainty and a fear of punishment if one ever exceeds what is permitted. The result can be hesitation or inaction that delays the arrival or the utilization of existing intelligence.

There is also, I believe, a responsibility on the part of congressional oversight to engage on this, partly in an effort to make sure the rules are understood and clear; to reassure officers that that they are expected to lean as far forward as the law permits; and that their efforts will be fairly judged by overseers who obviously share the commitment to keep the nation safe.

67123.750

Post-Hearing Questions for the Record
Submitted to the Honorable E. Thomas McNamara
From Senator Joseph I. Lieberman

"Ten Years After 9/11: A Status Report on Information Sharing"
October 12, 2011

1. In your prepared testimony you discuss the issue of "authorized use"– having the means to identify and validate the individuals who are using a system and providing them with access to information that is appropriate to their roles. The idea of an authorized use standard was a recommendation of the Markle Task Force in 2006. Efforts to implement such a standard have moved forward slowly in the last five years, but are receiving new attention in light of the Wikileaks disclosures of classified information.

   How important is it that we finally implement the concept of "authorized use" throughout our key intelligence and law enforcement systems? What are the key challenges associated with integrating this concept into these systems?

Answer:

Clearly, as with much of the progress in trhe ISE, authorized use started slowly, and it now needs to be pushed, accelerated, and completed by all agencies. It is most important that it be done, since without it, the ISE will not be fully mature and fully implemented.

As Program Manager, I initially favored a phased implementation, first within agencies, and then within each of the 5 communities (law enforcement, homeland security, defense, intelligence, and diplomatic), and a third stage including all agencies. To ensure that the results would be applicable government wide, I believe that the parameters of such a phased effort should be carefully coordinated, chiefly, by the Program Manager's office. I still support such a phased effort as the correct way to go.

I believe that the main challenges with implementing this concept are: bureaucratic inertia, resource constraints, and skepticism that it can work with effective security across all agencies. A certain, limited level of role-based suthorized use is being practiced in several agencies, and even within some communities. But, these are not, to my knowledge, simplified, standardized, and harmonized efforts that can be broadly applied within the ISE.

The time has come to establish a methodology and a timeline for full ISE implementation of role-based authorized use.

67123.751

GOVERNMENT OF THE DISTRICT OF COLUMBIA
METROPOLITAN POLICE DEPARTMENT

November 28, 2011

The Honorable Joseph I. Lieberman
Chairman, Committee on Homeland Security and Governmental Affairs
United States Senate
342 Dirksen Senate Office Building
Washington, DC 20510-6250

Dear Chairman Liebernan:

Thank you for the opportunity to appear before the Senate Committee on Homeland Security and Governmental Affairs at the October 12, 2011, hearing entitled: "Ten Years After 9/11: A Status Report on Information Sharing." The information below is provided in response to your follow up questions.

1. ***In your testimony you highlight the need to "institutionalize" information sharing, noting that "if this process is just built on relationships and personalities, there will be gaps and it will ultimately fail."In what specific areas do you believe that information sharing is overly dependent on personalities and relationships, such that it would be beneficial to further institutionalize information sharing?***

   There are several areas in which information sharing may still be dependent on relationships. For instance, communication of time sensitive classified information may not be available in advance of the development of classified bulletins unless an agency has established relationships or partnerships such as the Joint Terrorism Task Force. As I mentioned in my testimony, smaller law enforcement organizations are not equally engaged in information receipt or dissemination, largely due to lack of resources including staff with appropriate clearances that is dedicated to information sharing. This results in reliance upon relationships with fusion centers, task forces, or individuals who have access to classified information. Both our federal partners and large law enforcement agencies need to focus on institutionalizing outreach to these smaller agencies.

2. ***Your testimony discusses the role of the Washington Regional Threat and Analysis Center (the District of Columbia's fusion center) with respect to suspicious activity reporting. What is your assessment of the efforts that the federal government has made to facilitate and integrate the suspicious activity reporting process? Are there ways in which this process could be improved or streamlined?***

   The federal government, particularly the Department of Homeland Security (DHS), has provided tremendous assistance in developing a common tool for collecting Suspicious Activity Reports (SARs) and educational campaigns to raise awareness of the need to watch for and report suspicious activity. There is, of course, always room for progress. For example, it may be useful for the Department of Justice (DOJ) to clarify criteria for

P.O. Box 1606, Washington, D.C. 20013-1606

67123.752

submitting SARs to the National SAR Initiative (NSI) and eGuardian/Guardian, and to map Standing Information Needs (SIN) codes to SAR activity codes. Together, DOJ and DHS should ensure that SAR technology tools piloted by DHS and the Federal Bureau of Investigation are able to integrate with the NSI and eGuardian/Guardian. Collectively, the federal government should encourage more federal agencies to submit SAR data into the NSI, including the National Counter Terrorism Center, Terrorist Screening Center, Naval Criminal Investigative Service, Transportation Security Administration, the Defense Intelligence Agency, and others.

I hope you find this information helpful. Please do not hesitate to contact me if I can be of any further assistance.

Sincerely,

Cathy L. Lanier
Chief of Police

cc: Vincent C. Gray, Mayor, District of Columbia
Paul Quander, Deputy Mayor, Public Safety and Justice, District of Columbia

Post-Hearing Questions for the Record
Submitted to Captain Ronald E. Brooks
From Senator Joseph I. Lieberman

"Ten Years After 9/11: A Status Report on Information Sharing"
October 12, 2011

1. Your prepared testimony discusses the issue of sustaining funding for state and local fusion centers, and notes that this is a shared responsibility across all levels of government. Given the way that fusion centers are funded today, the extent to which the respective levels of government are providing funding or other resources is often unclear.

   a. What are fusion centers doing today, working with federal partners, to develop better data on current funding and allocation of resources?

   RESPONSE: The fusion centers in partnership with the DHS Office of Intelligence and Analysis (I&A) are taking steps to collect standardized data on budget sources and amounts. DHS created a questionnaire and sent it to each fusion center earlier this year. I understand that the vast majority of fusion center directors have submitted responses, and that I&A's analysis of the data will be available within the next couple of months. The National Fusion Center Association (NFCA) is well aware of the desire by DHS and Congress to have clarity on how many federal dollars are being invested across the National Network of Fusion Centers, and to have an understanding of the sources of those federal dollars. NFCA is working closely with I&A on this effort and has provided full support for efforts to develop a better under understanding of the aggregate funding picture. The challenge in quickly providing detailed budget information stems from the nature of the National Network – it is a decentralized, independently "owned" network of centers each of which is managed by different agencies at the state or local level. Each center has a different federal-state-local funding mix, but wer are moving forward on collaborative efforts to achieve clarity on that mix.

   b. What is being done or should be done to clarify federal responsibilities versus state and local responsibilities with respect to sustainment of fusion centers?

   RESPONSE: When we talk about sustainment of fusion centers, we are talking about maintaining and building the ability to leverage state and local resources to support federal homeland security efforts. To the extent the federal government would like to count on state and local connectivity to the community and the nearly 2 million public safety boots on the ground as force multipliers, federal responsibilities should include a reliable funding source that state and local governments can use to support fusion centers. That funding should support centers' efforts to sustain and build the four critical operational capabilities or

COCs (receive, disseminate, analyze, gather) relating to homeland security information, among other activities. In addition to federal grant support for COCs and fusion center operations, there has been substantial and much needed investment in the establishment of a standardized suspicious activity reporting process. Sustainment for the National Network also entails supporting this effort.

The NFCA recommends that Congress strengthen the Law Enforcement Terrorism Prevention Program or take similar actions to ensure that fusion center activities and true terrorism prevention activities are supported with federal grant dollars. In addition to grant funding, the continued contribution by DHS of trained intelligence officers to individual fusion centers is essential. Federal training resources should be made available to maintain and enhance the liaison officer program nationwide. This will ensure that the "front lines" of public safety are leveraged to the maximum possible extent in the detection and prevention of terrorism plots, and that the Nationwide SAR Initiative is fully implemented. State and local agencies will continue to sustain their investments in fusion centers, including through significant contributions of full-time personnel the economic value of which is not reflected in individual fusion center budgets.

2. Your testimony discusses the Nationwide Suspicious Activity Reporting Initiative. What is your assessment of the efforts that the federal government has made to facilitate and integrate the suspicious activity reporting process? Are there ways in which this process could be improved or streamlined?

RESPONSE: The NFCA believes the Nationwide SAR Initiative (NSI) is a foundation of joint federal-state-local-private sector homeland security efforts. It ensures that the eyes and ears of our highly trained, highly observant, and well-positioned corps of public safety personnel in every town, county, and state know what to do when they observe suspicious activity. And when that activity is reported, the Nationwide SAR Initiative ensures a standardized vetting process that has the protection of civil liberties at its core, and that ensures information flows to appropriate authorities as quickly as possible. Fusion centers are portals to the SAR process and are essential in effective NSI implementation, since they provide analytical capabilities and access to information systems in a standardized manner.

The NSI Program Office at the Department of Justice has been a very good partner and should continue to receive the support it needs for nationwide implementation. The NSI program mirrors the recommendations in IRTPA, specifically the implementation of a system that is decentralized and distributed, and the NFCA supports this approach.

67123.755

Fusion centers – better any other entity – are uniquely positioned to catalogue and assess critical infrastructure and other vulnerabilities. We can then layer in threat information provided by the FBI, DHS, and local sources, and SAR information reported through our network of trained liaison officers and by the public. Through analysis of that information, fusion centers can identify critical intersections, ensure that possible terrorism-related leads are referred directly to the JTTFs, and that other leads are channeled to the appropriate state, local, or federal agency for action in a timely manner.

With regard to NSI implementation, while much progress has been made there are still two U.S. Department of Justice-funded SAR reporting initiatives – the FBI's E-Guardian system and the NSI's Shared Space. I believe that while these two systems may be able to co-exist, under the current configuration there is a potential for loss of critical information and for misunderstandings related to privacy and civil liberties. I believe we must either adopt a single system for SAR reporting, or that the functionality of both systems must enable a single federated input and search capability. In any case we must continue to use the SAR vetting standard that is currently being used in Shared Space, and those standards should continue to be based upon known behaviors. Retention and redress should mirror what has been required by the Bureau of Justice Assistance and DHS in the fusion center privacy policies that are in force across the entire National Network.

67123.756

Post-Hearing Questions for the Record
Submitted to Jeffrey H. Smith
From Senator Joseph I. Lieberman

"Ten Years After 9/11: A Status Report on Information Sharing"
October 12, 2011

1. *In your testimony, you suggest that information sharing "is a tool that can help make the entire government more efficient." Do you have specific governmental missions or organizations in mind with respect to this recommendation, where the government might best apply lessons from the work that has been done on terrorism-related information sharing?*

The information sharing tools that have been developed for counterterrorism could help address other key national security priorities, such as the counterintelligence, cybersecurity, and counterproliferation missions.

However, information sharing is a means, not an end. The ultimate goal in each of these areas must be to dramatically change the way people responsible for counterintelligence, cybersecurity, and counterproliferation work together across agencies by using technology and the best management know-how to facilitate new forms of collaboration. This type of transformation can improve efficiency by increasing the flow of information and empowering people who are closest to the facts on the ground to quickly form teams that draw on experts with different backgrounds in government, academia, and the private sector. As these more powerful ways of sharing information are expanded to new missions, privacy and civil liberties protections must be increased simultaneously to keep pace.

Examples:

Counterintelligence - The Markle Task Force on National Security in the Information Age's recommendations regarding auditing and an authorized use standard can enhance the government's counterintelligence mission by improving our ability to identify and prevent insider threats. Implementation of real-time audits and immutable audit logs throughout the Intelligence Community would make it easier to identify the next Aldrich Ames or Robert Hanssen because these audits could reveal suspicious behavior. An authorized use standard could also limit the risk of government employees selling U.S. secrets to our enemies because they would have to establish that they were "authorized" to use the data based on their role, mission, and a predicated purpose.

These same tools could have helped prevent WikiLeaks' disclosure of hundreds of thousands of the State Department's diplomatic cables in 2010. The press has reported unusual behavior by Private Bradley Manning. Assuming those reports are correct, active audits could have flagged his behavior in real-time and he would likely not have had access to such a vast range of documents if SIPRNet had a dynamic permissioning system with granular access controls.

Cybersecurity - Best practices from counterterrorism information sharing could also potentially be employed to aid the cybersecurity initiatives that are being developed within the Departments of Homeland Security and Defense. Better information sharing tools can facilitate the flow of threat intelligence from the government to the private sector as well as private sector reporting of cyber attacks. Although the Markle Task Force has not had the opportunity to review the Defense Industrial Base Cyber Pilot that Deputy Secretary of Defense Lynn announced in June, in my view, the Pilot is an example of preliminary progress.[1] However, much more work is needed.

The same issues of trust that were critical to successful terrorism-related information sharing exist in the context of cyber attacks. Private businesses and critical infrastructure owners often fear that sharing information about exploitation of a vulnerability in their IT systems will harm their business. Much as the government's old "need to know" culture was an impediment to fusing disparate pieces of information about terrorists, this lack of trust in the cybersecurity sphere undermines cooperation that could prevent future attacks and provide a more comprehensive picture of the threat landscape. Moreover, traditional civil liberties must be protected as well in order to ensure that the American people trust the way our government is applying these tools to cybersecurity.

Developing a Plan to Apply Lessons Learned:

In my view, the President should designate an official, such as the Program Manager for the Information Sharing Environment or someone in the Office of Management and Budget, to develop a plan to apply the lessons learned from the work that has been done on terrorism-related information sharing to other national security missions. These lessons can transform the way our government tackles crosscutting national and homeland security issues.

Expanding these information sharing tools to new national security missions will not be easy. But, the post-9/11 reforms in the way our government answers the threat of terrorism demonstrate how much more effective government can be when new ways of working allow agencies, people and technology to collaborate in a more decentralized, public-private manner. As the ongoing economic instability and growing fiscal challenges heighten the need to reduce government's cost and improve its function, our progress in intelligence sharing since 9/11 points the way for government to do more with less.

---

[1] Dep. Sec. of Defense W. Lynn III, Remarks at the 28th Annual International Workshop on Global Security (Jun 16, 2011), *available at* http://www.cybersecuritymarket.com/2011/06/16/defense-industrial-base-dib-cyber-pilot/; Dep. Sec. of Defense W. Lynn III, Remarks at 2011 DISA Customer and Industry Forum (Aug. 16, 2011), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4863.

67123.758

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats
Chairman Joe Lieberman
October 18, 2011

Good morning, the hearing will come to order and thanks to our really excellent panel of witnesses for coming today to discuss the nation's record over the past decade in improving our defenses against a biological attack or a pandemic.

Today's hearing is part of our "10 years after 9/11" series assessing the status of a number of government homeland security operations that were singled out as inadequate or dysfunctional by the 9/11 Commission. The impetus for our review today as everyone will remember actually came a week after the 9/11 attacks, long before there ever was a 9/11 Commission, when our already traumatized nation was shaken anew by the mailing of anthrax spores to five news media organizations and two United States Senators.

All told, five people died from anthrax inhalation. Two were Postal workers. And one close to my home was a 94-year-old woman from Connecticut. Twenty-two others were sickened, and thousands – including some members of Congress and our staffs - took a course of powerful antibiotics to ward off possible infection.

We remember those days well around here because one of the letters was sent to Senator Daschle's office in the Hart building, where my office was and is located. The building was evacuated and closed for months while HAZMAT teams secured it. We were fortunate that no additional anthrax was found and no other attacks have occurred since. But that is unlikely to remain the case.

Three years ago, the Graham-Talent Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism concluded that a biological weapon was more likely than any other weapon of mass destruction to be used in an attack against our country. The Commission predicted such an attack would probably occur somewhere in the world within the following five years and concluded that the federal government was not prepared to respond adequately to such an event.

Last week, the Bipartisan WMD Research Center, which was a follow-on to that Graham-Talent WMD Commission, reported that the threat of a bioterror attack remains as strong as ever. We have no specific credible evidence I want to make clear that terrorists are now plotting such a specific attack. But they have made it very clear in word and action that they aspire to do so, and technological advances, I'm afraid, are making it easier, faster, and cheaper to accomplish such an attack.

So, the question today is, has the federal government developed the tools we need to respond effectively to a bioterror attack or naturally-occurring pandemic disease, to develop and disseminate vaccines and antibiotics, and to respond to the medical consequences that would result from such a biological disaster?

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.778

Over the past decade, we have spent billions of dollars on bio-defense research; on strengthening first responder capabilities; and on developing new vaccines, bio-surveillance systems, and forensic science techniques. Really we've done a lot more than the average American knows about to protect their security.

Our investments have resulted in a nation far more prepared to deal with a biological disaster we ever have been. Just yesterday the Connecticut Children's Hospital in Hartford conducted an exercise to test if it could immunize its employees within a 24-hour period in the event of a virus outbreak or bio terror attack. This is typical of preparedness at the local level which is going on all over the country and is absolutely key, and communities across the country have significantly improved their disaster planning since October 2001.

But it is also clear from reports that have been issued that we are not prepared for a catastrophic biological incident. We are much better prepared for a smaller WMD attack although gaps remain there too.

Since 9/11Congress has created a number of new offices and new technologies have emerged to improve security against a bio attack.

The Biomedical Advanced Research Development Authority (BARDA) – established at the Department of Health and Human Services (HHS) to fund WMD medical countermeasures -- has helped greatly increase our preparedness by delivering medical countermeasures to the National Strategic Stockpile, which now contains millions of doses of smallpox and anthrax vaccines; post-exposure therapeutics for anthrax, smallpox, and botulism; and some basic radiation treatments. As a result, our ability to treat victims with medical countermeasures has improved dramatically since 2001.

At the Department of Homeland Security (DHS), the National Bioforensics Analysis Center studies new bioforensic methods and identify the DNA of a biological agent so criminal investigators can pinpoint their source.

The Obama Administration also is tightening security at laboratories using the most dangerous pathogens and those most likely to be weaponized. I'm pleased to note that legislation which this Committee produced in October of 2009 helped facilitate this Administration action.

We have deployed—and I mention this for the benefit of the public--a network of aerosol sensors called Biowatch in cities around the country that's designed to detect anthrax and other biological agents. New technology is on the horizon that would shorten the amount of time that it takes the sensors to detect a bio threat.

These are significant advances, but they don't tell the whole story. Last week, the Bipartisan WMD Research Center concluded, and I quote: "Although [government] efforts have yielded considerable progress over the past decade, the nation does not yet have adequate bio-response capability to meet fundamental expectations during a large-scale biological event." End of quote.

We still, as far as I can determine, lack a strategy for dispensing vaccines and antibiotics in a mass crisis. We don't have the ability to track the spread of disease in real-time through a community or quickly reclaim contaminated areas to get people back to their homes and critical infrastructure up and running again.

67123.779

And 10 years after the anthrax attacks of 2001, we still do not have a more effective anthrax vaccine than the one developed in the 1950's. Medical counter measures for other chemical, biological, radiological, and nuclear threats have also not yet been developed.

Tight budgets have led to an under-staffed medical surge force to respond to a biological attack in communities around the country. In fact, right now discussions are underway in Congress to eliminate funding for programs that coordinate the overall medical response to a bio attack, such as the Metropolitan Medical Response System, and for centers that train public officials in emergency response.

So DHS, HHS, and FBI, working together and in coordination with state and local governments, and the private sector, have an enormous responsibility to continue to work to increase our capability to protect the public from deadly biological attacks. This Committee has been working with federal agencies to make sure that they can fulfill that responsibility, and we will continue to work with in that direction to make sure they can do so in a way that's ever more effective.

So we've come a long way. Perhaps we'll never be as fully protected as we'd like to be, but we have a ways to go. I'd like to focus on both sides of that story and look at what we've done as well as what we still have to do.

67123.780

Statement of
Senator Susan M. Collins

Ranking Member, Homeland Security and Governmental Affairs Committee

Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats

October 18, 2011

It has been a decade since the anthrax attacks that left five people dead and 17 sickened.

It has been just two weeks since the operation in Yemen killed Anwar al-Awlaki, who reportedly sought poisons including cyanide and ricin to attack the U.S.

The new leader of al Qaeda has a medical background, raising concerns that he may have an even greater interest in pursuing chemical and biological terrorism.

Since 2001, more than $65 billion in federal funds have been invested in biodefense, but progress has been difficult to quantify.

With the growth of new technologies and online road maps, terrorist groups may soon be able to threaten nation states with biological weapons. And, some countries, like Syria, have never ratified the Biological Weapons Convention.

Former Senators Bob Graham and Jim Talent issued their report on the prevention of WMD proliferation and terrorism in 2008 and predicted the use of a weapon of mass destruction in a terrorist attack by 2013. They found it more likely that a terrorist group would be able to obtain and use biological weapons than nuclear, and they continue to sound the alarm. Just last week, they issued a "report card" grading improvements in detection and diagnosis capabilities, medical countermeasures availability, and communications.

They found stagnation on medical management and on the development, approval, and dispensing of medical countermeasures. Think of this Committee's investigation into the difficult time the Administration had in distributing the flu vaccine to respond to the naturally occurring H1,N1 outbreak.

The Administration received F's from the commission in areas such as attribution of even small-scale events and environmental cleanup of large-scale incidents. This is not acceptable.

To safeguard our citizens against bioterrorism, we must have the ability to respond effectively after an attack has occurred. But we do not yet have adequate bio-response capability to meet fundamental expectations during a large-scale biological event. The WMD Prevention

67123.781

and Preparedness Act that Senator Lieberman and I introduced in 2009 would have established a detailed plan for preventing and responding to a biological attack.

A biological attack is especially worrisome because we likely would not immediately know that we had been attacked.

That is why I am concerned about the effectiveness of the BioWatch Program. Secretary Napolitano has touted this nationwide environmental monitoring system designed to detect the intentional release of aerosolized biological agents. According to the GAO, however, a threat agent may not be identified until more than a day after its release.

While the next-generation of BioWatch technology could bring this down to just four hours, we are not yet certain that this technology will be viable.

In addition to technological upgrades, better coordination between DHS and HHS is necessary to enhance our ability to identify a threat agent quickly and to increase the speed and reliability of attribution so that we can prevent follow-on attacks.

Ultimately, our best hope of detecting and containing an attack is the low-tech, unglamorous but critically important system of intelligence combined with a robust public health surveillance network. This is still the most effective system and we must be careful not to look for technological "magic bullets" to relieve us of the duty to maintain and strengthen our public health surveillance.

The Graham-Talent Commission also found serious flaws in the security of biological labs in our own country.

A 2009 GAO report, which I requested, reported alarming deficiencies in basic perimeter security at facilities that house the world's most dangerous biological pathogens, like the Ebola and smallpox viruses. GAO also found that laboratory regulation "for the most part relies on self-policing."

While security controls must be improved within our own country, global security problems are even more daunting. The crossroads of terrorism and proliferation, biology and technology, in volatile countries such as Pakistan are troublesome.

A multitude of federal agencies--DHS, EPA, HHS, CDC, USDA, and the FBI, among others-- all have some responsibility for bioterrorism. It concerns me that so many different federal entities could be scrambling to respond during and after an attack. And, of course, state and local health officials and first responders are part of the system as well.

Yet, the Executive Branch does not have one agency or official that is the designated leader on all elements of biodefense, especially the coordination and dissemination to both law enforcement and public health stakeholders of critical intelligence.

This is a major gap in our prevention and response capability. If we cannot tell our health providers what to look for when there is a potential threat, we can't properly trigger the public health surveillance system that is our best hope for early detection, containment, and response.

We need a leader who can direct the response and eliminate overlap or redundancy. This official should have the ability to coordinate across federal agencies and harness the assets and expertise of state and local governments, first responders, and the private sector.

I look forward to discussing how we can strengthen our nation's biological defenses and security systems.

U.S. Senate
Committee on Homeland Security and Governmental Affairs
Testimony of the Honorable Tara O'Toole, M.D., M.P.H.
Under Secretary for Science and Technology Directorate
Department of Homeland Security

October 18, 2011

Introduction

Good morning Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. It is an honor to appear before you today to discuss the state of U.S biodefense ten years after letters containing *Bacillus anthracis* or "anthrax" killed five people and sickened seventeen others and to report on the biodefense portfolio within the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T). In the decade since the Amerithrax incident there have been significant gains in the country's ability to detect, respond to and recover from a deliberate bioattack or a natural epidemic of infectious disease.

Designing and implementing a viable biodefense is a complex undertaking. U.S. efforts to date have engaged multiple Federal agencies, national laboratories, state and local governments, first responders, the medical and public health communities, the private sector and individual American households. International biodefense collaborations involving U.S. allies are underway. President Obama and Secretary Napolitano regard biosecurity as a top national priority. The President's recent address to the U.N. General Assembly urged all nations "to come together to prevent, detect and fight every kind of biological danger – whether it is a pandemic like H1N1, a terrorist threat, or a treatable disease."[1][2]

Overview of Biological Defense Programs at the Science and Technology Directorate

Since its creation in 2002, the Department of Homeland Security's Science and Technology Directorate (DHS S&T) has made many contributions to US biodefense in the form of knowledge products (analyses, standards, assays), new technologies and technical tools and through participation in various Interagency processes. S&T's efforts have been especially focused on:

- Biothreat studies - deepening our understanding of the specific biothreat agents of greatest concern to better focus national preparedness and response activities,
- Detection and Identification of bioagents -developing science-based strategies, practices and technologies required for the timely detection of covert biological attacks, including the development and fielding of the original Biowatch technology, and the precise identification of biothreat agents,

[1] Obama, Barack. "Remarks by President Obama in Address to the United Nations General Assembly." United Nations Headquarters. New York, New York. 21 September, 2011.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01166 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.784

- Environmental remediation and area recovery - determining feasible and effective means of identifying and remediating the environmental contamination left in the wake of bioattacks,
- Essential Biodefense Laboratory Infrastructure - building and operating national laboratories essential to biodefense, such as the National Biodefense Analysis and Countermeasures Center (NBACC), the Plum Island Animal Disease Center (PIADC), and the National BioAgro Defense Facility (NBAF),
- Biodefense for Agriculture - conducting, in collaboration with the US Department of Agriculture (USDA), front line research in biodefense of US agricultural assets, including the development of diagnostics, medicines and vaccines relevant to foreign animal diseases
- Bioforensics - establishing a sound technical and operational basis for conducting forensic investigations of bioattacks and biocrimes.

DHS S&T staff have been highly active participants and leaders in numerous, ongoing Federal Interagency efforts to advance US biodefense. I co-chair the National Science and Technology Committee on National and Homeland Security, along with Mr. Zack Lemnios of the Department of Defense (DoD) and Phil Coyle, Associate Director of the White House Office of Science and Technology Policy. Our scientists serve on 32 Committees and Working Groups across the interagency. These working groups and committees examine the full range of biodefense issues from dual-use research, bioterrorism threat intelligence, and first responder detection CONOPs, to diagnostics and the development of medical countermeasures (MCM). These efforts involve all of the executive branch partners including Department of Health and Human Services (HHS), USDA, DoD, Department of Justice, and Environmental Protection Agency (EPA).

While there are still important challenges ahead of us, these extensive efforts have resulted in a government and citizenry considerably more prepared to respond to and recover from a biological attack than we were a decade ago. DHS S&T has been an important part of this progress. Building upon the work started in the national labs and other federal agencies, S&T has crafted a portfolio that addresses the full continuum of the threat. My testimony will provide an overview of the bioterror threat and DHS S&T's biodefense work.

The Bioterror Threat is Real and Will Grow as Bioscience Advances

Ten years after anthrax was mailed to members of the U.S. Congress and to media organizations, dozens of policy, intelligence, and technical reports have affirmed the viability of terrorist groups using biological weapons to cause death, suffering, and socio-economic disruption on a calamitous scale. In 2008, the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism stated that it, "…is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013." S&T has worked diligently to increase understanding of the full spectrum of potential threats and their consequences.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01167 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.785

More than a decade ago, the Defense Science Board affirmed that, "there are no technical barriers to a large-scale bioattack."[2] We are living in the midst of a biotechnology revolution where the knowledge and tools needed to acquire and disseminate a biological weapon are increasingly accessible. It is possible today to manipulate pathogens' characteristics (e.g. virulence, antibiotic resistance), and even to synthesize viruses from scratch. These procedures will inexorably become simpler and more available across the globe as technology continues to mature. Thankfully, the combination of technical expertise required and the restrictions limiting the acquisition of the materials necessary for production still make this a challenging task.

Even small-scale attacks could be highly lethal and disruptive, and as has been noted, there is a real possibility of a campaign of bioattacks on multiple targets (the "reload" phenomenon) – because these weapons are self-replicating organisms. Moreover, it is not necessary for a nation-state to maintain a large stockpile of bioweapons to pose a significant asymmetric threat as the development of a significant offensive bioattack capability could occur within weeks or months.

DHS S&T Biothreat Studies

Understanding the biological threat and the relative risk posed by biological agents is a fundamental need for any biodefense capability. Homeland Security Presidential Directive 10: Biodefense for the 21st Century, DHS S&T has the responsibility to conduct the Biological Terrorism Risk Assessment (BTRA) every two years. The BTRA has been developed in partnership with experts in the law enforcement and intelligence communities, along with input from the scientific, medical, and public health communities, and serves as a starting point for biodefense investment priorities.

The BTRA is a comprehensive, strategic-level assessment designed to 1) aid in identifying and prioritizing credible, high impact threats, 2) aid in identifying and prioritizing vulnerabilities and knowledge gaps, and 3) provide a systematic, science-based, common framework for "what if" analyses. At its core, the BTRA is a model. It does not predict the future, but provides a way to think logically, using common assumptions, about more and less likely possible futures. The BTRA approach encompasses a wide variety of possible attack scenarios to ensure that the assessment outcomes are comprehensive. Consider the scope of the 2010 study which examined:

- 4 types of terrorists (international, state-sponsored, domestic, lone wolf) exploiting
- 43 different bioagents (38 human, five livestock pathogens) that may be obtained from
- 2 locations (foreign and domestic) by
- 5 routes of acquisition (among them theft and environmental isolation) with
- 6 methods of production and weaponization to attack
- 20 different targets (including a subway, stadium, transportation or outdoor events) using
- 8 modes of dissemination (e.g. food, aerosol) causing exposure by
- 2 routes (inhalation or ingestion) resulting in
- 3 public health consequences (illnesses, fatalities, and economic consequences).

[2] Defense Science Board, *Biological Defense*, June 2001; p.18.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01168 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.786

The end result is millions of enumerated scenarios of what is possible in bioterrorism. To date, S&T has conducted BTRAs in 2006, 2008 and 2010. Additionally, S&T conducts companion analyses such as the Chemical Terrorism Risk Assessments (conducted in 2008 and 2010), the Radiological and Nuclear Terrorism Risk Assessment (conducted in 2010) and the Integrated Terrorism Risk Assessments (conducted in 2008 and 2010). These risk assessments are used by other Federal departments and agencies to guide their CBRN response planning.

The strength of the BTRA is due in large part to the work conducted by the National Biological Threat Characterization Center (NBTCC). This unique, national-level S&T asset was created by DHS in 2004 as part of the NBACC to address gaps in our knowledge related to high priority biological threat agents and to help support decisions regarding biodefense resource prioritization. The NBTCC performs scientific experiments to address the critical knowledge gaps related to acquisition, production, and dissemination in order to ensure an effective knowledge base for critical decision making in biological defense.

The most significant utilization of the BTRA is its role in providing risk input in shaping the multi-million dollar MCM investment decisions of the HHS. The Project BioShield Act of 2004 outlines the multi-step process utilized by DHS and HHS to ensure that the nation's MCM research, development, and acquisition activities are grounded in a risk-based process. In summary, as identified in the BTRA, the bio-agents which present the greatest risk to the U.S. population are further analyzed in a Material Threat Assessment (MTA) process led by DHS's Biodefense Knowledge Center, located at Lawrence Livermore National Laboratory. During the MTA process, DHS evaluates the intelligence and threat information for top priority agents and develops and models a "highly plausible" consequence scenario includes the number of potentially exposed individuals. The MTAs are provided to HHS, which then conducts further analysis to determine public health impacts. DHS and HHS work collaboratively to review all of these data and determine if an agent poses a significant national security threat. Based on these deliberations, the Secretary of Homeland Security issues a Material Threat Determination (MTD).

To date, DHS has issued 11 MTDs for biological agents, two MTDs for classes of chemical agents, one MTD for radiological materials, and one MTD for nuclear detonation effects. The MTD is a statutory requirement for procurements using BioShield funds; however the issuance of an MTD does not guarantee that the government will pursue countermeasures against that agent. If an MCM is sought, DHS has a statutory responsibility alongside HHS in recommending to the Office of Management and Budget to release the BioShield Special Reserve Funds.

Biological Surveillance, Detection, and Diagnostic Capabilities

Early indication of a biological attack is very challenging due to the dual-use nature of the required knowledge and materials and the small size of operational footprint necessary to produce the agents making detection difficult. In the absence of pre-attack interdiction, it is crucial that the U.S. has the means to detect and mitigate an attack either through large-scale technology programs such as BioWatch or through enhancing the capabilities of First Responders and Public Health professionals by, for example, the creation of better methods for

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01169 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.787

detecting bioagents in the field or conducting reliable lab analyses. Other S&T investments also work to create sensors which could automatically initiate protective actions (e.g. altering a building's airflow patterns) as well as develop rapid diagnostic capabilities as both a means of detection and a critical element to help mitigate an attack by guiding our response.

Standard Field Protocol for Rapid Resolution of Suspicious White Powders: Since 2001, responses to incidents involving suspicious "white powders" have impacted the First Responder community; these events are often costly and disruptive. S&T has invested in tools to both reduce the cost and impacts of these responses and to standardize the responses to ensure that any real events are optimally handled.

S&T has led an interagency effort with the Center for Disease Control and Prevention (CDC), Federal Bureau of Investigation (FBI), EPA and National Institute of Standards and Technology to develop multiple standards on bulk and swab sample collection of suspected biothreat powders and operational guidelines for initial response to a suspected biothreat agent to ensure that the procedures and sampling strategies used are effective and support confirmation and prosecution if a real incident were to occur. These standards were published by the American Society for Testing and Materials, an international standards organization in 2010. These standards are increasingly being adopted by First Responders and are already in use by multiple states and the FBI.

Rapid Portable BioDetector for First Responders: S&T is developing technology intended to evaluate suspicious powders in the field in a matter of minutes. Although laboratory confirmation is the only way to reliably determine the presence of a biological organism, this technology will help emergency responders assess a threat.

Detect to Protect (D2P): Current biodetection systems are designed to "detect to treat". Studies done by S&T of bioattacks and chemical attacks on subways and by DOD at the Pentagon show that bio-aerosols can spread throughout a subway system or building very quickly. These investigations highlight the need for very rapid, tight connections between initial detection of a release and response actions. Such "detect to protect" systems are challenging to build, because they must balance the need for a fast detection against the fact that fast detection sensors are prone to false alarms.

To address these difficulties, S&T is pursuing a multi-tiered bio-aerosol DP2 program for sensing a bioattack within metro systems, airports, buildings, and stadia. Low cost, rapid "trigger" sensors when tripped immediately initiate "behind the scenes" protective actions to slow spread of an agent, such as changing air flows within a space while turning on a confirmation sensor. The confirmation sensors are high confidence detection technologies provide the high confidence analysis necessary to support high-impact actions such as building evacuations or warnings to shelter in place or alerting of public health officials. Such a multi-tiered detection approach not only helps reduce the spread of the agent and the extent of human exposure in near-real time, but could also reduce system costs by decreasing the required number of expensive confirmer sensors. S&T is currently conducting operational tests and evaluations on the D2P system within the Boston Metro (Massachusetts Bay Transportation Authority – MBTA).

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01170 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.788

Assay development and standards: A key element of any successful detection or diagnostic tool is the assay which provides the ability to discern the unique molecular signatures of an agent. DHS S&T has a highly robust bioassay program that is focused on the development of improved assays as well as standards and test methodologies to foster confidence in deployed detection systems. Some of the aspects of assay development currently ongoing include:

- Efforts that focus on the creation of highly specific assays with the ability to differentiate microbes at the sub species. This is important because different sub species will have very different impacts on human health. This level of resolution is essential information for public health officials.
- The recent development of a rapid Ricin Detection Assay with extremely high specificity and sensitivity. This assay is currently undergoing its final validation study and is anticipated to be deployed through the Center for Disease Control and Prevention's (CDC) Laboratory Response Network (LRN) before the end of the calendar year.

DHS S&T has led the interagency in the development of standards that guide the appropriate levels of sensitivity and specificity needed for assays deployed in various environments. There are generally two levels of standards for assays, one for use by First Responders when making decisions to evacuate buildings or close off streets, and another used by the CDC to declare medical emergencies and issue medications. Working with the Association of Analytical Communities and their Stakeholder Panel on Agent Detection Assays S&T developed the consensus standards for Public Safety Actionable Assays (PSAA) to support the testing and validation of commercial technologies that might be used by the First Responders in the field. A much higher standard of performance is needed for those assays designed to be used by the CDC LRN when making high-impact public health decisions such as the distribution of antibiotics. At the request of the White House in Fiscal Year 2008, S&T has been working with our Interagency partners including the CDC, DoD, State and Local public health authorities to develop the Federal Standards for Assay Performance and Equivalency (FSAPE) which specifically aims to ensure a common standard for sensitivity and specificity for assays that will be used to make public health actionable decisions. This process is nearing completion and has already received the buy-in from multiple stakeholders in the public health community.

Any bio-detection architecture needs to be a coordinated effort leveraging multiple federal laboratories for sample analysis and public health decisions. S&T led in the establishment of the Integrated Consortium of Laboratory Networks (ICLN) to serve this purpose The ICLN coordinates a network of laboratories that, in the case of an act of bioterrorism, will be accountable for provision of timely, credible, and interpretable data in support of surveillance, early detection, and effective consequence management. By coordinating Federal labs, the ICLN can take a risk-based approach to events and minimize capability gaps of individual labs.

Advanced Biodiagnostics: Currently, there are no approved, point-of-care clinical diagnostic tests that physicians could use to determine if an individual is infected with a bioterror threat agent. The traditional diagnostic approach involves blood culture analysis which requires one or more days to deliver results. In situations where outcomes depend on rapid treatment after

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01171 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.789

exposure, or in mass casualty situations where scarce resources must be deployed intelligently, the ability to rapidly identify infected victims is a strategic necessity. DHS S&T, in partnership with the DoD Defense Threat Reduction Agency, the National Labs, and the CDC, are pursuing an effort to develop a broad-spectrum diagnostic with the potential to identify exposure to biological agents prior to the onset of symptoms.

Rapid Test for Antibiotic Susceptibility: DHS S&T, in collaboration with the CDC, has developed a rapid assay to determine antibiotic susceptibility for *B. anthracis* and *Y. pestis*. These rapid assays reduce the timeline for answers by 50% compared to the gold standard conventional susceptibility assay. Given that some of the biothreat agents possess very short incubation periods for disease onset and are coupled with high mortality rates after symptomology, the need for rapid antimicrobial susceptibility assays is critical.

Response and Recovery from Bioattacks

Much of our national biodefense investment focuses on detection of and medical treatment for a biological attack. However, it is equally essential to develop capabilities, protocols and technologies that support rapid attribution to identify the source of the attack as well as help an impacted area quickly and appropriately respond to and recover from an attack

Bioattack response and recovery operations are complex and much work remains to be done in this arena. The Environmental Protection Agency (EPA) has the lead in the area of environmental restoration but it is widely acknowledged that the EPA budget is too small to support a robust program. DHS S&T, as well as DoD, have made strategic investments in this area and several of the efforts have yielded valuable insights that I would like to bring to your attention.

Responding to an Attack: S&T's biodefense investments include the development of guidance and technologies to diminish uncertainty and enhance data-driven decisions in the hours and days after an epidemic is first detected. Immediately following a bioattack there will be a critical need for "situational awareness" - information leaders will need to guide the response - but reliable data will be hard to obtain quickly with current systems, technologies, biosurveillance capacities and communication flows. During the initial days following a covert attack, there is likely to be significant uncertainty regarding whether the observed epidemic is natural or deliberate, the scale of the attack, where the attack occurred; who was exposed; whether the bioagent is susceptible to specific antibiotics, whether and where the environment is contaminated, whether and where there might be additional attacks, etc.

Viable Particle Capture Device: This program is developing a low-cost deployable device that continuously samples the air and collects and stores any airborne particles or pathogens in a manner that keeps them viable for laboratory analysis. Because of the low-cost nature of the device it can be widely deployed throughout a city as an augmentation of the BioWatch network and after an attack has been detected the additional sample points would greatly increase the knowledge of where an agent had been dispersed. Even more importantly, the device ensures that any agent collected during an attack is viable allowing laboratories to identify it and test it for virulence and anti-biotic resistance.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01172 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.790

Multi-Application Multiplex Technology Platform (MAMTP): The testing systems currently in use at the Laboratory Response Network labs that process the BioWatch samples were designed around the public health mission and are not optimized to support a Biodefense surveillance system in terms of the number of agents that can be tested and throughput. The MAMTP is a technology platform that will be able to perform up to 100 tests or detect 100 targets simultaneously within a single sample. The platform will use a standardized cartridge system to reduce costs and aid in surge capacity which will be needed to handle the thousands of samples that will be collected after an attack in an effort to identify where the agent has spread.

Anthrax Re-aerosolization: A significant question with regard to anthrax attacks is whether the anthrax bacteria, which are unusual as they are protected by an extremely hardy spore coat that makes it resistant to environmental degradation, could become "re-aerosolized" and continue to pose a health threat once it is deposited on surfaces following the initial attack. The answer has significant implications for remediation strategies, but existing data is limited and contradictory. DHS S&T, in partnership with DoD, EPA and the national labs, is conducting studies to understand this problem within urban areas. These studies will address gaps in our understanding and will inform key policy decisions for evacuation vs. shelter-in-place, distribution of medical countermeasures, clean-up, and re-occupancy.

Recovery from an Attack: It is essential that the Nation have the capability to rapidly restore buildings, public infrastructure and critical utilities to full-function after an attack. This need is especially pertinent in the context of anthrax, because of the long-lived nature of this microbe, but understanding the extent, duration and consequences of post-attack contamination needs to be further explored.

Interagency Biological Restoration Demonstration (IBRD): This interagency effort included partnerships with state and local governments in the Seattle Urban Area and was co-funded with the DoD's Defense Threat Reduction Agency. The IBRD program developed a Seattle Region Plan for determining approaches for response and restoration activities, which served as the foundation for the development of the "Interim Consequence Management Guidance for a Wide-Area Biological Attack" document that can be used by other cities.

Mass Transit System Biological and Chemical Dispersion Studies: S&T studied releases of simulated biological and chemical agents in the Boston subway and DC metro systems to determine how material would move, disperse, deposit and could be mitigated through fast acting detection systems and changes to the airflow control systems. This effort is being continued through a partnership with the Washington Area Metropolitan Transit Authority to conduct simulated attacks on the Metro system to develop response protocols and above-ground countermeasure requirements.

Bioforensics: In 2001, there existed numerous challenges associated with microbial forensics investigative capabilities. Among them were no biocontainment lab, staff or equipment singly dedicated to microbial forensic analysis and limited evidence handling processes peer-reviewed analytical methodologies, or quality guidelines. Today, S&T owns and operates a national asset for biological forensics and attribution, the National Bioforensics Analysis Center (NBFAC), which is part of NBACC, was established by HSPD10 as "the lead Federal facility to conduct

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01173 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.791

and facilitate the technical forensic analysis and interpretation of materials recovered following a biological attack in support of the appropriate lead Federal agency." S&T owns and operates this national asset for biological forensics and attribution.

The NBFAC provides 24/7 support for biocrime and bioterror investigations for the Federal Bureau of Investigation (FBI), DHS Customs and Border Protections , the U.S. Secret Service and other government agencies with dedicated staff, equipment and biocontainment laboratories designed specifically for bioforensic analysis. The NBFAC has developed sensitive and specific assay capabilities for more than 60 bacterial, viral and toxin agents and has processed over 8,000 samples and completed 137 cases in support of Federal Law Enforcement agencies. The NBFAC also maintains a Bioforensic Reference Repository collection of geographically and temporally diverse biological agents to support comparative forensic analyses. The NBFAC trains FBI examiners to safely handle biologically contaminated evidence and supports traditional forensic exams. As a result of NBFAC, the U.S. can now do in days to weeks what previously required months.

Construction of the National Bio- and Agro- defense Facility

S&T was charged by Congress to design and build the National Bio- and Agro-defense Facility (NBAF), a laboratory with the capacity to perform research and development work on large animals at the highest (BSL-4) laboratory biosafety containment levels. After an extensive three year competition and evaluation, Manhattan, Kansas was selected as the site for NBAF. Since 2009, Congress has appropriated $154 million for NBAF design, site preparation and construction. The state of Kansas has pledged to contribute $110 million towards construction costs and has donated land for the site. The total remaining cost of NBAF construction was estimated as of 2011 to be $874 million. Construction of this facility, which is an essential part of the US biodefense infrastructure, is dependent upon continued support from Congress.

For more than 50 years, the Plum Island Animal Disease Center (PIADC) has served as the primary US laboratory facility for conducting vital livestock disease research. Despite its many successes, the age of PIADC facilities, its limited capacity restricts research and is impeding the development of needed countermeasures. PIADC has no capacity to do research at the Biosafety Level 4 (BSL-4), the highest bio-safety level, which is essential to combating the most dangerous animal disease threats. Currently, the U.S. must rely on partnerships with large animal BSL-4 labs in Australia and Canada. In the event of a bioattack on agriculture, or an attack employing a zoonotic disease, the U.S. would be unable to do the research needed for response. PIADC has no surge capacity for response to wide-scale events and its island location off the coast of New York limits operations in adverse weather conditions. Failure to build the NBAF will not only place the security of US agriculture in jeopardy, but would seriously impair U.S. scientific eminence in this important field.

S&T's R&D efforts are subject to ongoing review

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01174 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.792

Biodefense is just one of the many areas addressed by S&T's diverse portfolio. To ensure that individual R&D projects are meeting the goals established by our partners in the operating components and the broader homeland security enterprise (HSE), S&T has committed to an annual review of our portfolio of basic and applied R&D and all proposed "new start" projects. The review process consists of written materials, an oral presentation by the project manager, and careful analysis of the project's likely impact and feasibility (or "riskiness") as judged against specific metrics determined by S&T with input from the operating components. These metrics are designed to address elements essential to programmatic success in the context of the DHS's QHSR missions, namely:

- *Impact:* Is our portfolio making a significant impact on our customer's mission?
- *Transition:* Are we transitioning relevant products to the field?
- *Technical Positioning:* Is our investment positioning the organization for the future?
- *Customer Alignment:* Are our projects aligned with well-understood customer requirements?
- *Customer Involvement:* Do we have the appropriate level of customer interaction?
- *Innovation*: Are we sufficiently innovative in the way we approach our challenges?

A review panel of S&T leaders, the DHS Component representatives, and outside experts evaluates and rates each project. By measuring all of our projects against this framework, we will provide a transparent and "shareable" view of all R&D within S&T; enable more strategic, longer-term budget decisions; ensure efficient delivery to the component or end user; and nurture effective communication throughout the process. This particular review model has been used by both Federal and private R&D organizations, including the prize-winning Army Engineering, Research and Development Laboratory. Review is key to ensure that S&T remains focused on the highest priority challenges in biodefense and ensuring that our work is complementary, not duplicative, of other agencies.

Challenges Remain for Biodefense

The design and implementation of a robust, cohesive, and cost-effective biodefense system will be the work of a generation. Despite the significant gains made over the past decade, much work remains to be done to deal with today's – and tomorrow's – challenges. As President Obama has noted, true biodefense against both deliberate and natural epidemics of infectious disease must be an international endeavor.

In the coming years, the DHS S&T Directorate intends to focus its resources on developing capacities to detect bioattacks in near-real time in order to enhance protective response actions. There will also likely be calls to improve detection of a wider range of potential threat agents, including genetically altered, synthetic or unanticipated agents, and possibly to enable detection of food and surface contamination. Faster, more detailed and reliable characterization of bioevents to improve situational awareness and inform response will be necessary. We must continue to develop an agile approach that accommodates possible epidemics of emerging disease or attacks using unforeseen bioagents or agents not addressed by stockpiled countermeasures. Inexpensive, real-time, point-of-care diagnostics will be essential to enabling

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01175 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.793

rapid identification and treatment of those at risk from epidemic disease and to containing the spread of contagious disease. Strategies for coping with and stopping bioterror campaigns must be developed. Mechanisms of international cooperation in dealing with infectious disease outbreaks and collaborative approaches to financing and refining needed biodefense technologies and countermeasures must evolve.

It is critical to understand that bioscience is in a state of revolution. Advances in our understanding of living systems and our technological ability to manipulate these systems are proceeding globally at a breathtaking pace. The biothreat landscape of the next ten years will not resemble today's. The technologies, tools and capabilities being developed need to be viewed not just through the lens of today's threat agent list, but from the perspective of capabilities available to our adversaries in the future.

Thank you for the opportunity to appear before you today. I am happy to answer any questions you might have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01176 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.794

Written Statement of Alexander G. Garza, MD, MPH
Assistant Secretary for Health Affairs and Chief Medical Officer
U.S. Department of Homeland Security
Before the Senate Homeland Security and Governmental Affairs Committee
October 18, 2011

Chairman Lieberman, Ranking Member Collins, and distinguished members of the Committee: thank you for inviting me to testify before you today. Secretary Napolitano highlighted a number of Department of Homeland Security (DHS) activities related to efforts to prepare for and protect against biological attacks in the 2011 Progress Report reviewing DHS and partner efforts to build a country that is stronger, safer and more resilient. I welcome this opportunity to discuss how the Office of Health Affairs (OHA) contributes to this effort.

I would like to begin by providing an overview of OHA and our role within the Homeland Security Enterprise. OHA serves as DHS's principal authority for all medical and health issues. We look at health through the prism of national security, providing medical, public health, and scientific expertise in support of the DHS mission to prepare for, respond to, and recover from all threats. OHA's responsibilities include serving as the principal advisor to the Secretary and FEMA Administrator on medical and public health issues; coordinating DHS biological defense programs; providing medical expertise to support DHS preparedness and response efforts; and leading the Department's workforce health protection and medical support activities. OHA also serves as the primary DHS point of contact for state and local governments on medical and public health issues.

The threat of a biological attack is real and challenging. As you know, the Weapons of Mass Destruction (WMD) Commission reported that we must be vigilant in addressing several urgent threats, especially bioterrorism. Additionally, the Quadrennial Homeland Security Review (QHSR) identified high-consequence biological attacks as a priority threat.

A wide-area attack using aerosolized *Bacillus anthracis*, the bacteria that causes anthrax, is one of the most serious mass casualty threats facing the U.S. A successful anthrax attack could potentially expose hundreds of thousands of people, and cause illness, death, fear, societal disruption and economic damage. Even a small scale attack, such as the Amerithrax attacks of a decade ago, will result in deaths, panic, and economic losses, making this a weapon of mass disruption as well as destruction. The time between exposure and the administration of medical countermeasures (MCM) is the most critical parameter in determining the extent of how many lives are lost in a biological attack.

Since the anthrax attacks 10 years ago, the Department has made progress in protecting the nation from biological attacks, and preparing the nation to respond to such events. OHA lends our expertise to a number of initiatives across the Department that focus on the threat of a biological attack.

67123.795

The federal government recognizes two critical capabilities must be in place to minimize the effects of a biological attack. First, we must be able to rapidly determine that an attack has occurred. Second, we must have the capability to quickly distribute MCM to the affected population before clinical symptoms appear. This timeline can be as short as one to two days. OHA manages a number of programs and activities designed to improve the government's capabilities in both of these areas.

Detection

One of OHA's primary responsibilities is to mitigate the consequences of biological incidents through early detection. Traditional epidemiological surveillance is too delayed to mitigate large scale attack consequences. Therefore early detection is a key tool to make the Nation more resilient against catastrophic health events. Prompt identification of a biological attack has the potential to increase the speed of delivery of medical countermeasures and save lives.

OHA's BioWatch program is a federally-managed, locally-operated, nationwide bio-monitoring system designed to detect the intentional release of aerosolized biological agents. This program deploys collection devices and analytical capability in more than thirty high-risk metropolitan areas throughout the nation. The intent of the BioWatch program is to provide public health experts with a warning of the presence of a biological agent before those who are exposed develop symptoms of illness. This "detect-to-treat" approach gives public health officials an opportunity to respond as quickly as possible in order to mitigate the potentially catastrophic impacts on the population. BioWatch uses risk information provided by the Bioterrorism Risk Assessment (BTRA) developed by the DHS Science and Technology Directorate to inform which agents to detect.

In addition to, and equally import as, providing critical early detection capabilities, the BioWatch program has built a collaborative capacity among the federal government, state and local public health, and emergency management communities that did not previously exist. This partnership is a model of interaction where a rapid, unified response is required.

To become more effective and efficient in detection of threat agents, in 2010 the Department began testing the next generation of automated early-detection systems, known as Generation-3 (Gen-3). Current detection capabilities, termed Gen-1/2, consist of outdoor aerosol collectors whose filters are manually retrieved for transport to and subsequent analysis in a Laboratory Response Network (LRN) facility. This system, while extremely beneficial, is labor intensive with results potentially not available until 12-36 hours after the release of a biological agent. The transition to an automated detection system (Gen-3) is designed to improve the time to detect to 4-6 hours, increase population coverage, and provide greater overall cost effectiveness. Shortening the time to detect is critical because it allows responders more time to distribute countermeasures to the affected population. Therefore this investment in Gen-3 has the potential to greatly enhance our capability to mitigate the effects of a biological attack. Gen-3 field testing

67123.796

was recently concluded in Chicago, and operational testing and evaluation is scheduled to begin in one city this fiscal year, and three additional cities in FY13.

Biosurveillance

Another key element to our approach to addressing biological threats is comprehensive situational awareness of potentially harmful biological events. OHA is focused on developing and maintaining an integrated, near real-time, multidisciplinary common biosurveillance picture that provides the Federal government and state/local partners with an accurate assessment of potential and unfolding biological events which can be used to better inform mitigation and response decisions.

To that end, OHA manages the National Biosurveillance Integration System (NBIS)—a consortium of federal partners that was established to rapidly identify and monitor biological events of national concern. NBIS collaborates among Federal and state partners to collect, analyze, and share human, animal, plant, food, and environmental biosurveillance information as well as threat information to provide early warning and situational awareness of a possible biological attack or pandemic. By identifying those bio-events that have reached reporting thresholds and publishing reports using the Biosurveillance Common Operating Picture (BCOP), the National Biosurveillance Integration Center (NBIC) and NBIS enhance recognition of biological events of national concern, reduce response time, support better decision-making, and promote effective response.

While the NBIC and NBIS have been successful in helping us to achieve our biosurveillance mission, there is still much more work to do to achieve a true national capability. OHA is currently partnering with our stakeholders to enhance and improve the NBIC while successfully meeting the statutory requirements and Congressional intent. We will continue to work to increase collaboration and data integration, improve analysis, and ensure high-quality, timely reporting.

Response and Recovery

OHA works directly with the Department of Health and Human Services (HHS) and state and local public health, emergency management and emergency medical services leaders to develop capabilities to respond to health security threats, including those posed by biological threats. We have done this by expanding local public health participation in, and coordination with, the national network of fusion centers. Specifically, OHA helped develop a resource document for state and major urban area fusion centers that identifies the recommended actions for fusion centers to integrate the public health and medical communities into the fusion process. Furthermore, we develop guidance for health and medical experts to better access federal grant and training programs to improve public health preparedness capability.

OHA provides health and medical expertise to planning and exercise efforts that advance national preparedness and response capabilities for threats that have potential health

67123.797

consequences. The Anthrax Response Exercise Series (ARES), which we completed in partnership with FEMA last fall, is an example of this work. The workshops included federal, state, regional and local public health and emergency management professionals and were designed to help coordinate roles, responsibilities and critical response actions following a wide-area anthrax attack. This year we plan to continue to build on the success of ARES by conducting workshops in additional high-threat cities.

In addition to ARES and other exercise activities that allow state and local governments to strengthen their national response capabilities, OHA also sees its role as providing our state and local partners with guidance for protection of personnel. Through the federal interagency process, OHA continues to lead the effort to develop consensus guidance regarding appropriate protective measures for responders in the immediate post-attack environment of a wide-area aerosolized anthrax attack. This guidance will reflect the most current understanding of the unique environment that would exist after a wide-area anthrax release. DHS and its Federal partners are committed to continually updating the guidance to ensure that it reflects the most recent policy and technical developments.

In April 2010, DHS established the Anthrax Preparedness and Response Steering Committee to coordinate and focus Department preparedness and response efforts to an anthrax attack. The Steering Committee leads the Department's efforts in enhancing readiness and immediate response in the event of a wide-area aerosolized anthrax attack and includes senior leaders from across the Department. A number of products have been developed under the leadership of the Steering Committee, including response playbooks and checklists, guidance for newly-elected officials, and exercise protocols to broaden attention to biological defense.

Furthermore, OHA works to provide Department leaders with appropriate subject matter expertise in public health, medicine, food defense, agricultural security, veterinary defense, pandemic influenza preparedness, and other threats. Our Food, Agriculture, and Veterinary Defense (FAVD) Branch initiative leads the coordination of the Department's programs to ensure the security of our nation's food, agriculture, human and animal health. FAVD experts support the Department's efforts to enhance preparedness through capabilities development and facilitate the integration of the emergency management services community into federal, state, local, territorial, and tribal food and agriculture sector disaster preparedness activities.

Medical Countermeasures

As discussed earlier, our biodefense activities are aimed at mitigating the effects of a biological attack through early detection and ongoing surveillance. Early detection allows communities to provide MCM to affected persons in a timely manner to protect lives. OHA coordinates routinely with our Federal partners, especially HHS, including the Office of the Assistant Secretary for Preparedness and Response (ASPR), the Centers for Disease Control and Prevention (CDC), and the Food and Drug Administration (FDA) on medical countermeasures issues and represents DHS as a member of the HHS-led Public Health Emergency Medical Countermeasures Enterprise (PHEMCE).

67123.798

On December 30, 2009, President Obama signed Executive Order (E.O.) 13527, "Establishing Federal Capability for the Timely Provision of Medical Countermeasures Following a Biological Attack." The E.O. sought to mitigate illness and prevent death, sustain critical infrastructure, and complement state, local, territorial, and tribal government MCM distribution capacity. OHA participated in a number of interagency and interdepartmental efforts aimed at addressing the requirements of the E.O.

Section 2 of the E.O. directs the development of a National United States Postal Service (USPS) MCM dispensing model for U.S. cities to respond to a large-scale biological attack. In collaboration with the Departments of Justice (DOJ), Defense, HHS, and USPS, DHS supported the development of the USPS model, which was submitted to the National Security Staff on June 30, 2010. Upon request, DHS will work with DOJ who leads the coordination of Emergency Support Function (ESF)-13 to provide required law enforcement support for the U.S. Postal model in those jurisdictions considering this modality of distributing MCM.

Section 3 of the E.O. directs the development of a federal rapid response capacity to supplement state and local governments and the private sector's capabilities to deploy MCM. This effort was co-led by FEMA and HHS, with OHA being a critical partner in providing subject matter expertise during the development of this Federal Interagency Concept of Operations Plan—Medical Countermeasures Dispensing (FICOP – MCM). This concept plan was submitted to the NSS in September 2011. This work culminated in a table top exercise in Los Angeles, California, led by FEMA's National Exercise Division on September 8, 2011. This focused discussion brought together federal, state, and local officials to enhance biological preparedness by codifying common expectations regarding the federal concept to support initial state and local MCM dispensing. The exercise was well received and information gained helped to finalize the FICOP-MCM. FEMA is now developing a regional operations plan to support the greater Los Angeles area, and we expect that federal operational planning will expand to other metropolitan areas as well.

Section 4 of the E.O. directed federal agencies to establish mechanisms for the provision of MCM to personnel to ensure that the mission essential functions of the executive branch departments and agencies continue following a biological attack. In addition, the Department and HHS have the responsibility to develop a plan to provide MCM directly to mission-essential personnel to ensure continuity of operations. OHA leads this effort for DHS and the Department is among the first federal agencies to have met this requirement of the E.O.

DHS Workforce Health Protection

OHA works each day to build resilience across the country and also within the Department. We do so by leading and strengthening our nation's collective efforts to secure our country from the threats we face. We also build resilience by ensuring the protection of our workforce.

67123.799

As discussed earlier, in Section 4 of the E.O., the President ordered the federal government to establish mechanisms for the provision of MCM to personnel performing mission-essential functions. Secretary Napolitano further directed the Department to develop a plan to provide emergency antibiotics to all DHS employees in an attack area, not just those who are mission-essential.

The DHS workforce includes a wide variety of mission-essential personnel who work in varying geographical locations throughout the U.S. and internationally. Due to the nature of DHS workforce's security mission, some DHS personnel could be exposed during response activities or while performing their duties each day at airports and ports of entry.

Survival is increased if individuals exposed to biological agents take antibiotics quickly. This underlies the importance of the Department's plans to pre-position MCM in caches across the country for employees. Existing community plans will also provide support to DHS employees and their families.

OHA spearheaded the MCM strategy for DHS employees and oversees the purchase and storage of MCM for the DHS workforce. The MCM strategy and implementation plan is a multi-year, multi-layered approach, each building upon the previous to achieve its goal of covering the entire DHS workforce. The focus of our MCM effort for the DHS workforce thus far has been stockpiling anthrax antibiotics, and will expand in the future to protecting against other biological threats. This scalable approach will ensure the sustainability of the program.

Since the program's inception, we have purchased courses of anthrax MCM and stored them at a central location as well as regional locations. OHA, in coordination with DHS components, identified accessible and secure facilities for storage of the anthrax MCM. Additional cache locations will be identified over time to improve coverage and proximity to employees. OHA also built points of dispensing capability to dispense MCM as needed by providing training to appropriate personnel.

We also provide medical guidance and logistical and operational support to DHS component offices as they finalize their MCM plans. OHA has also provided medical guidance in the form of Standard Operating Procedures, including for storage of MCM, administration of MCM for anthrax spore exposure, non-medical points of dispensing for MCM, and working and service animal anthrax spore exposure. OHA now has mechanisms in place to verify the medical credentials of DHS personnel who will provide the medical oversight of MCM storage and dispensing.

Conclusion

I would like to conclude by thanking this committee for your continued support of OHA's mission and for your guidance. Thank you again for the opportunity to testify today. I look forward to your questions.

67123.800

Testimony
Committee on Homeland Security and Governmental Affairs
United States Senate

Safeguarding our Nation: HHS Readiness to Respond to a Biological or Other Emergency

Statement of
Nicole Lurie, MD, MSPH
Assistant Secretary for Preparedness and Response
U.S. Department of Health and Human Services

For Release on Delivery
Expected at 10:00am
Tuesday, October 18, 2011

67123.801

Good morning Chairman Lieberman, Ranking Member Collins, and Members of the Committee. I am Dr. Nicole Lurie, the Assistant Secretary for Preparedness and Response (ASPR) at the U.S. Department of Health and Human Services (HHS). Thank you for inviting me here today, on behalf of HHS, to testify on our nation's public health preparedness for a biological event.

Ten years ago, letters containing anthrax spores were mailed to several offices in Congress and the news media. While we were ill prepared at the time to face those attacks, we have made steady and significant progress over the past decade in our capabilities to prepare for and respond to such events. We have learned many lessons from subsequent events and continue to identify, improve and refine our capabilities. Thanks to investments made by Congress and the guidance that we continue to receive, we have made significant improvements in preparedness, response, and recovery at the federal, state, and local levels and have invested in a number of medical countermeasures to respond to a chemical, biological, radiological, or nuclear threat. State and local partners are more prepared than ever before, due to enhanced response capabilities, improved coordination, and enhanced awareness among the public health and medical communities. We have new legal and policy tools including statutes that created the Office of the ASPR to oversee a national program, and programs elsewhere that bolstered our nation's defenses against a chemical, biological, radiological, or nuclear (CBRN) event.

67123.802

One of the biggest challenges we have encountered in the last decade is the lack of common national approaches and effective coordination among governments, health and response systems, and communities. The September 11, 2001 attacks in New York, Pennsylvania, and Washington D.C., and Hurricane Katrina offer particularly poignant examples of challenges and the imperative to improve. While there is still a lot of work ahead of us, we have made great strides in developing a unified national direction in strategy, policy, planning, and operations. Today, we have the National Response Framework and the National Recovery Framework to guide collective efforts to respond to and recover from disasters and emergencies, from the smallest incident to the largest catastrophe. In 2009, HHS released the National Health Security Strategy (NHSS), which refocuses the patchwork of disparate public health and medical preparedness, response, and recovery strategies to ensure that the nation is prepared for, protected from, and resilient in the face of health threats. The NHSS is the first strategy focused specifically on protecting people's health during an emergency, and has a vision built on resilient communities and strong, sustainable health and emergency response systems.

Our resilience depends on shared responsibility for preparedness across governments – from local communities to global partners, and includes all members of the public as full and equal partners in health security. Looking back, I'm encouraged by how far we have come and by how we are working together now in planning for the future. Challenges do however remain. The

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01185 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.803

threats to national security and public health are real and are constantly evolving. As science and technology create new opportunities for useful advances, they may also lead to new threats. As I testify today on our readiness, I will address both specific progress we've made over the past decade and the strategies we have in place to ensure that we continue to improve in advancing toward our goals.

In 2001, the use of anthrax spores in a biological attack killed five people, infected 17 others, threatened thousands more, and resulted in billions of dollars in costs—forcing us to re-think our approaches to preparedness for the CBRN threats that we face. Collectively, we recognized that we lacked basic capabilities and that a long-term concerted effort would be required to close the preparedness gap. Since that time we have also learned that investment alone is not enough—and in response we have established a common set of investment priorities and have fundamentally changed the way we manage our medical countermeasure enterprise. As Secretary Sebelius noted in 2010, "our nation must have the nimble, flexible capability to produce medical countermeasures rapidly in the face of any attack or threat, whether known or unknown, novel or reemerging, natural or intentional."

The nation owes a debt to the Congress in this context for providing critical authorities and appropriating billions of dollars for development and procurement of CBRN medical countermeasures that have been turned into real products by

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01186 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.804

the combined efforts of the National Institutes of Health (NIH), the Biomedical Advanced Research and Development Authority (BARDA), Food and Drug Administration (FDA), and the Centers for Disease Control and Prevention (CDC). This includes an unprecedented investment in pandemic influenza preparedness—what we often think of as a model approach in addressing a threat. I can say with certainty that we are now more prepared for the range of CBRN threats and other emerging infectious diseases, such as pandemic influenza, than at any point in our nation's history. For example, while prior to 2005 the country had lost its capability to domestically manufacture vaccines for the threat posed by a novel avian influenza, we have reversed the trend and are on the verge of having a fully approved manufacturing capability in partnership with Novartis for not just a brand new domestic manufacturing plant, but a completely novel and agile manufacturing process for this vaccine. Thanks to the foresight of Congress, the Project BioShield program, and the Public Health and Emergency Medical Countermeasures Enterprise (PHEMCE), we have products in the Strategic National Stockpile (SNS) for smallpox, anthrax, botulism, and radiological and nuclear threats. And, as we crossed the "valley of death" in advanced development, we have had substantial success with the medical countermeasure pipeline – including over 80 candidate products that if successful have the potential to transition to procurement contracts and inclusion in the SNS including. These include an entirely new class of antibiotics; anthrax vaccine and antitoxins; smallpox vaccine and antivirals; radiological and nuclear countermeasures including hematopoietic, radionuclide, pulmonary, cutaneous,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01187 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.805

and gastrointestinal candidates; pandemic influenza countermeasures; and the first set of chemical antidotes. Furthermore, in demonstration of our end-to-end approach to development, we have successfully moved a product through all phases of the medical countermeasure pipeline—from discovery to procurement—and have begun manufacturing a new smallpox vaccine (Modified Vaccinia Ankara). We also developed and produced 186 million doses of 2009 H1N1 vaccine in record time for use in the U.S. and for international donation. However, there remain both complex scientific, financial, and marketplace challenges. In recognition of the need to do better, in December 2009, Secretary Sebelius requested a review of the medical countermeasures enterprise to ensure the nation has a forward-looking, 21st-century enterprise system upon which it can rely during an emergency or other public health event. In August 2010, HHS released the Public Health Emergency Medical Countermeasures Enterprise Review: Transforming the Enterprise to meet Long-Range National Needs (MCM Review). The MCM Review focuses on "processes, policies, and infrastructure required to take a product concept derived from a national requirement through research, early and advanced development, manufacturing, regulatory approval, procurement, and stockpiling." Specifically, this review examined the steps involved and made recommendations regarding the research, development, and regulatory approval of medications, vaccines, and medical equipment and supplies for a public health emergency. As detailed in the 2011 Bipartisan WMD Terrorism Research Center's Bio-Response Report Card (WMD Report Card), medical countermeasure development and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01188 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.806

procurement faces significant challenges due to the issues related to coordination of budget requests across our multiple agencies and availability of "sufficient, sustained funding." One recommendation included in the MCM Review was implementation of an integrated approach across the Department for investments in research, development, and procurement of medical countermeasures. FDA, NIH, ASPR, and CDC are currently working on a consolidated 5-year investment plan for such investments which will focus on many of the coordination issues regarding budget requests.

It is important to note that we are also working collaboratively with our interagency partners at the Department of Defense (DoD) to ensure appropriate synergy in our medical countermeasure activities and to avoid costly duplication of efforts, where possible.

The WMD Report Card also mentions HHS' efforts to build an advanced development and manufacturing facility to increase the national capacity for rapid manufacturing of pandemic influenza vaccines and other products during an emergency. I am pleased to inform you that HHS has contracts with multiple manufacturers to produce influenza vaccine annually. We have also entered into a contract supporting a cell-based approach to developing vaccine and have retrofitted other facilities to enhance domestic influenza vaccine manufacturing capacity.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01189 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.807

Critical to our continued success is active and thoughtful partnership with the private sector. As you know, the federal government is often the only purchaser of essential preparedness products. In 2001, only a small sector of entrepreneurial companies ventured into the development and manufacturing of needed CBRN medical countermeasures. That remains true today. In response, the MCM Review includes two new initiatives. First, the Strategic investor (SI) is designed to support promising start-up companies with a full suite of testing, evaluation, product development, and manufacturing services, and the other is designed to provide meaningful financial incentives and rewards to private sector partners who succeed in developing the medical countermeasures we need. The Strategic Investor program is requested in the President's Budget, and we are working closely with the Congress to establish it in the reauthorization of the Pandemic and All-Hazards Preparedness Act. In addition, we have moved forward on the Centers for Innovation in Advanced Development and Manufacturing (CIADM) program and we look to make awards early in 2012. Both programs offer an opportunity to leverage limited federal resources and incentivize new participation in this business sector, as well as look toward a process that can help this sector realize sustainability by creating products using platforms that can be applied to commercial and government needs. In addition, in 2008, we reviewed internal contracting processes and reorganized the line of reporting to reflect a more appropriate and efficient organizational structure consistent with comparable business models in the U.S. government. We established targets and timelines for contracting processes and aligned them

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01190 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.808

with a set of triggers. These actions and our close coordination with stakeholders helps to ensure that contract terms are clarified and requirements are better understood from the start. We are also using Broad Agency Announcements (BAA) to support investments in research and development of medical countermeasures. These BAAs have expedited review of proposals and contract awards immensely.

We know that leveraging our existing regulatory and scientific capabilities will ultimately lead to a more robust pipeline of products. The MCM Review prioritizes the translation of medical countermeasures concepts and research as well as enhances regulatory innovation, science, and capacity. Specifically, we need to ensure that the discoveries NIH supports through its investments in basic science are cultivated and available to be turned into products whose potential utility we may not yet appreciate. In addition, targeted investment is needed for regulatory science at FDA in order to increase their capability to respond to new technologies for which they are mandated to regulate, and to help them provide greater clarity to sponsors and manufacturers about the pathways to product approval.

In addition to these new tools and approaches, we established an enterprise-wide approach to management of the MCM portfolio. The Public Health Emergency Medical Countermeasures Enterprise (PHEMCE) serves as the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01191 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.809

overarching interagency convening body to coordinate the multiple efforts and programs that enable the nation to have the medical countermeasures needed to respond to CBRN and other emerging infectious disease threats. ASPR leads the PHEMCE, which brings together three primary HHS agencies—NIH, CDC, and FDA—along with four key interagency partners—Department of Homeland Security (DHS), DoD, Department of Veterans Affairs (VA), and Department of Agriculture (USDA). Working together, full-time, as an enterprise, these agencies and organizations are coordinating, exchanging information, and learning from each other daily to optimize preparedness and response for public health emergencies in connection with the creation, stockpiling and use of medical countermeasures. As a result of the 2010 MCM Review and based on development and procurement accomplishments, PHEMCE partners are now working to release an updated Public Health and Emergency Medical Countermeasures Enterprise Implementation Plan for Chemical, Biological, Radiological, and Nuclear Threats, expected in 2012. The current plan was developed in 2007 and has served as a playbook to guide research and procurement. The updated plan will continue to guide and coordinate investments across the spectrum of research, development, and procurement.

Beyond the realm of medical countermeasure development and procurement, HHS has a critical role in response operations. Since the tragic events of September 11, 2001, we have experienced a number of incidents impacting public health that have required a coordinated response to save lives. These

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01192 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.010

events—from hurricanes to emerging infectious diseases—each presented unique challenges. We have successfully captured the lessons learned from each operation and incorporated the concepts into subsequent planning and response operations. There continue to be a number of challenges, including reductions in state and local public health and medical resources and a continued need to more effectively coordinate with federal, state, local, tribal, non-profit, and private partners. In addition, we have recognized that new approaches are needed. These approaches must increase our focus on an all-hazards approach; improve our planning to ensure that funding is available when it is needed in an emergency; include conversations with the response community about crisis standards of care; and incorporate at-risk populations and behavioral health considerations into all aspects of our response planning.

Recently, we have seen tangible evidence of the value of our efforts and investments at the federal, state, and local level. The federal response enterprise is greatly strengthened, as evidenced by a robust National Disaster Medical System, expanded surveillance capabilities and deployable public health teams, and a Strategic National Stockpile with $4.4 billion worth of medical countermeasures at its disposal. Since 2001, HHS has expanded the Secretary's Operation Center (SOC) to ensure all public health and medical communications are coordinated and communicated to all stakeholders before, during, and after a public health incident. We are harnessing technologies to aid in response efforts, using electronic medical records to match demand with need,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01193 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.011

geographic information systems to identify demographic characteristics of affected populations and available resources, and social media to communicate with new audiences and gain information on developing health trends.

Beyond these new technologies, there have been great improvements at the state and local levels including investments in hospital and community preparedness, establishing response plans for all-hazards, and conducting no-notice drills to test capabilities. A number of recent natural disasters were adequately managed at state and local levels; 10 years ago I am not confident this would have been the case. These incidents include the flooding in the Red River Valley and the tornadoes that touched down in Alabama and Missouri. In each incident, states were better able to respond and required little or no federal support. For example, Missouri purchased a mobile medical unit just before St. John's Regional Medical Center was destroyed by a tornado in May 2011. This mobile medical unit is still in use today providing the residents of Joplin essential medical care. However, this does not mean we can 'check the box' on adequate state and local response capability. The financial realities we all face challenge our public health and medical infrastructure and will further widen gaps in our laboratories, emergency rooms and public health departments. Two critical tools available to support investments in preparedness are the Hospital Preparedness Program (HPP) and Public Health Emergency Preparedness (PHEP) cooperative agreement programs. HPP and PHEP support efforts at state and local public health and medical facilities to ensure that communities are prepared to respond

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01194 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.812

to public health emergencies. With HPP grants, we have made great strides in the ability of the predominantly private sector health care system to surge to provide medical care to large numbers of patients. In fact, more than 76 percent of hospitals participating in the HPP met 90 percent or more of all program measures for all-hazards preparedness in 2009. This is a significant accomplishment and clearly demonstrates participants' commitment to investing in preparedness. PHEP funding has fostered an increased level of preparedness throughout communities and contributed to state and local governments' decreased reliance on federal aid following disasters. We have made impressive strides as a nation in our state and local public health capabilities. There was a time in the not too distant past when getting internet access for a local health department was a challenge; the concept of sending blast fax communications was seen as a progressive and novel idea.

While we have made great strides in preparing state and local communities and public and private healthcare facilities, without continued support and funding for our public health and medical system, the infrastructure could begin to degrade and health outcomes may be affected. We are already witnessing a decline in the public health workforce as a result of fiscal constraints. As state and local capacity diminishes, we could see an increase in the call for federal assistance in response to disasters. This could result in longer recovery periods, higher response costs, and greater potential for loss of life.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01195 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.813

As you know, I joined ASPR in 2009 and was immediately faced with a global public health emergency—a novel pandemic influenza virus. Due to the foresight and planning of the federal government and the Congress, we had developed an unprecedented level of preparedness for this emergency. At that time, we were three years into a five-year pandemic influenza plan and had allocated significant time, energy, funding, and resources in order to diversify domestic vaccine production and surge capacity; advance development of influenza vaccines manufactured in cell culture, antigen-sparing adjuvants, new antiviral drugs, and point-of-care clinical diagnostics; stockpile medical supplies and ventilators; and expand international surveillance, research, and scientific collaborations. In addition, we had successfully strengthened our national laboratory capacity to provide enhanced epidemiologic support quickly to detect emerging public health incidents. These are clear examples of prior investments paying off during real world events.

In each of our response efforts – from hurricanes and floods to earthquakes and infectious diseases – we have witnessed the importance of all-hazard planning. Since we are limited in our ability to forecast new and emerging threats, we are modifying response plans to ensure they are nimble, flexible, and adaptable to new challenges. All response operations require the commitment of resources as soon as possible to save lives. In today's budget environment, it is important to ensure resources are available to support a response as soon as a need arises. If we were to face another emerging infectious disease event similar to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01196 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.814

the H1N1 pandemic, it is important to be able to quickly obligate funds to contracts to ensure adequate manufacturing of vaccine and antivirals to treat the population and limit spread. We are promoting a culture of budget preparedness across the federal, state, local and private sectors to ensure we are able to quickly and efficiently get resources where they are needed for the earliest critical response to a disaster.

We have always known that faster responses lead to better health outcomes. After our response to the Haiti earthquake we implemented actions to: streamline internal operations to ensure providers are adequately supported; provide needed services quickly and efficiently following disasters; and, ensure we have access to information that supports surveillance of the spread of illness. We have moved forward to improve the timeliness of information gathering and sharing, deployment times and distribution of countermeasures and other equipment and materiel. More recently, however, we have initiated systems to improve our responses before they even occur. In just this past year, FDA issued an emergency use authorization permitting pre- and post-event preparedness activities for mass distribution and dispensing of doxycycline in the event of an anthrax attack. This action will reduce the time it takes to provide a life-saving medical countermeasure to the end user in the event of an attack. We have also worked to strengthen the National Disaster Medical System (NDMS). NDMS is a federally coordinated system that augments the Nation's medical response capability. NDMS utilizes an Electronic Medical Record (EMR) system

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01197 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.815

that is able to standardized record keeping and promotes enhanced health surveillance during disasters. We are able to use the EMR system to better identify population needs, specifically in the area of pediatrics. The ability to identify the needs of the population, specifically the pediatric and at-risk population, will support a better and more focused response in the future.

It is critical that we include at-risk populations in all planning models and during the development and procurement of medical countermeasures. HHS has taken steps to ensure that at-risk individuals—children, pregnant women, senior citizens and other individuals who have special needs—are included in all planning scenarios, guidance documents, plans, and will be effectively treated in the event of a public health emergency. During the 2009 H1N1 pandemic, surveillance identified distinctly different risk groups—especially children and pregnant women—who quickly became, and remained, priority subgroups for prevention and mitigation measures, including vaccination and school closures. Identifying and monitoring this population was important in reducing the spread of illness. Finally, we include provisions for pediatric studies in every Project BioShield contract to support eventual licensure of products for this population.

So far I have addressed how we have improved and continue to improve enterprise management of our medical countermeasures and response efforts. As we move forward in those areas, we also need to be thinking about the foundations in thought that underpin all of our planning across preparedness,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01198 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.816

response, and recovery—how to foster needed scientific research and build the evidence base for everything we do. One of the biggest challenges in preparedness and response has been the lack of a strong knowledge base to support decision-making, inform the public, and allow for rigorous assessments and continuous improvement in progressing toward our goals. One compelling example is from the 2010 Gulf oil spill. One of the public's primary concerns during this incident was, understandably, whether oil and dispersants would negatively affect their health and the health of their families and loved ones. We did not have adequate science or the best mechanisms in place to collect data during the response. Taking this as an important lesson learned, we have made significant progress. The NIH National Institute of Environmental and Health Sciences (NIEHS) has established studies and a research consortium with partners to address different health aspects of the oil spill and impacts on the affected communities, including looking at workers' exposure to oil and dispersants. HHS is also participating in a group of 17 federal agencies led by NOAA to create a single shared data repository and virtual workspace for federal agencies and the larger research community to access health data collected during the oil spill. The spill also offered an important reminder that nearly every emergency or disaster has a health impact or a need to communicate with affected communities about health concerns. Therefore, we are working to ensure that HHS and our partners are appropriately involved at the early stages of any national response.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01199 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.817

As I conclude, it is important to recognize that despite the deaths of Osama bin Laden and Anwar Al-Awlaki, threats to the nation—and specifically to our public health—will continue. There continues to be real threats from the deliberate use of chemical, biological, radiological, or nuclear agents by hostile states or terrorists. In addition, the threat of natural disasters and emerging infectious diseases with the potential to cause widespread illness will always remain. We are actively working to improve based on the number of challenges and events we have faced. Looking forward, there are also improvements for which we need your support. I applaud Congress' wisdom in enacting the Pandemic and All-Hazards Preparedness Act (PAHPA) in 2006 that authorized my office and provided us needed authorities to enhance efforts to prepare for and respond to public health and medical incidents. As you work to reauthorize PAHPA, I encourage you to consider provisions that support getting the right resources, whether countermeasures or healthcare professionals, to where they are needed in an emergency; ensure adequate medical countermeasures are available for dispensing as soon as possible following the start of a public health incident; establish more efficient reimbursement for our partners following public health incidents; and reauthorize critical expiring authorities. We must continue investing in development of medical countermeasures, novel approaches to response operations, and our public health infrastructure. The reauthorization of PAHPA supports our work and will ensure we continue to have the tools necessary to respond.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01200 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.818

Ultimately, all of our investments and efforts come down to the same goals – building a resilient nation and saving lives when disaster does occur. We have made great strides toward building a robust enterprise to quickly get medical countermeasures to people who need them, incorporating the clinical community into national preparedness systems and preparing clinicians to treat patients affected by emergencies, and collaborating with state and local partners to develop, exercise, and improve their response capabilities. I look forward to working with you to ensure that this progress and our strategies for the future continue to prepare the nation and save lives. Thank you for the opportunity to testify before you today. I am happy to answer any questions you may have at this time.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01201 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.819

STATEMENT FOR THE RECORD OF
VAHID MAJIDI
ASSISTANT DIRECTOR
WEAPONS OF MASS DESTRUCTION DIRECTORATE
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"TEN YEARS AFTER 9/11 AND THE ANTHRAX ATTACKS: PROTECTING AGAINST BIOLOGICAL THREATS"

PRESENTED
OCTOBER 18, 2011

Introduction

The Federal Bureau of Investigation's (FBI) number one priority is to protect the United States from terrorist attacks. Within that priority, the threat of Weapons of Mass Destruction (WMD) is the FBI's most pressing concern. WMD terrorism and proliferation are evolving threats to United States national security. The Director of National Intelligence has assessed that dozens of identified domestic and international terrorists and terrorist groups have expressed their intent to obtain and use WMD in future acts of terrorism. Indicators of this increasing threat include repeated ambitions and actions of terrorists and criminals to acquire materials and knowledge related to WMD. The challenge presented by these threats is compounded by the large volume of hoax threats that distracts and diverts significant resources from law enforcement agencies.

FBI Weapons of Mass Destruction Directorate

The FBI is the lead law enforcement agency responsible for investigation of WMD threats. In particular, the FBI has authorities relating to the investigation, prevention, and response regarding individuals that attempt to obtain or use WMD materials, technology, and expertise. In the past, several FBI Headquarters (FBIHQ) divisions provided oversight and coordination on WMD matters. In 2004 the 9/11 Commission recommended that FBI create a new specialized and integrated national security branch to include agents, analysts, linguists, and surveillance specialists to cover the counterterrorism and counterintelligence missions. The WMD Commission Report, generated in response to the anthrax mailings, echoed this recommendation and the FBI responded by creating the National Security Branch (NSB). In 2005, the FBI Director assigned the newly-formed NSB to design an operational element to meet the WMD threat. The Weapons of Mass Destruction Directorate (WMD Directorate; WMDD) was

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01202 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.820

created in July 2006, consolidating WMD investigation and prevention efforts to create a unique combination of law enforcement authorities, intelligence analysis capabilities, and technical subject matter expertise focused on chemical, biological, radiological, nuclear and explosive matters. Over the last five years, WMDD has developed and refined capabilities in the areas of investigations, operations, countermeasures, intelligence analysis, training, and oversight of the WMD Coordinators (FBI Special Agents that manage WMD-related matters in each of the FBI's 56 Field Offices). Additionally, the WMDD maintains detailees at the International Criminal Police Organization (INTERPOL), the Republic of Georgia, and Singapore for international coordination.

WMDD's primary mission is the prevention of WMD terrorism and proliferation through proactive programs. Unlike many threats the FBI has historically encountered, WMD threats have the potential for major disruption at a national level, with catastrophic impacts. For this reason, WMDD leadership places emphasis on the prevention of incidents, and mitigation of threats. Specifically for biological WMD and bioterrorism, WMDD programs and initiatives are aimed at preventing, detecting, deterring, and disrupting the acquisition, production, and utilization of biological agents against the homeland.

Timely and relevant intelligence supports the FBI's proactive approach to countermeasures, investigations, and operations. The FBI contributes to and consumes intelligence products to establish a clear picture of emerging and imminent threats at strategic and operational levels. With a more thorough understanding of the threats, vulnerabilities, and risks in each area of responsibility, WMDD better prioritizes resource requirements and targets initiatives in the needed areas.

The preparedness component of the WMDD mission incorporates planning, training, and exercises to ensure the FBI and its US Government (USG) partners are ready to respond to WMD threats. This involves the development of comprehensive plans and policy at the strategic and operational levels that specify responsibilities and courses of action for all involved. Countermeasures bolster policy, and include outreach activities, identification of key indicators, and other measures to counter or eliminate the WMD threat. They supplement the intelligence information and enable WMDD to address the WMD threats before they happen.

If a WMD threat materializes, the FBI has the responsibility to investigate the threatened, attempted, or actual use of a WMD, as well as the attempted or actual transfer of materials, knowledge, and technology needed to create a WMD. The FBI maintains and manages a strong response capability to collect evidence in contaminated areas, disarm hazardous devices, and provide direct command and control support for critical incidents.

FBI Authorities

The FBI is the lead Federal Agency responsible for the investigation of bioterrorism and biological crimes, including the threatened, attempted, or actual use of a

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01203 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.821

WMD and the attempted or actual transfer of knowledge, materials, and technology to produce a WMD. The most relevant biological WMD statutes are 18 USC §2332a, 18 USC §175, 18 USC §175b, and 18 USC §1038. 18 USC §2332a states it is unlawful for any person without lawful authority who knowingly uses, threatens, or attempts or conspires to use a WMD. 18 USC §175 makes it illegal for any person without lawful authority to knowingly develop, produce, stockpile, transfer, acquire, retain or possess any biological agent, toxin, or delivery system; and 18 USC §175b adds it is illegal for a restricted person to ship, transport, possess, or receive a select biological agent or toxin in or affecting interstate or foreign commerce. The FBI also has the authority to investigate WMD-related intent to relay false or misleading information and hoaxes, as derived from 18 USC §1038.

The Threat

Over the past decade, the potential for biological terrorism has not diminished. The FBI assesses that some of those who plan to attack the homeland or US interests abroad are interested in using biological agents or toxins to achieve their goals. Documents discovered at Tarnak Farms confirmed Al-Qa'ida's active program to obtain biological seed stock. Terrorist groups such as Al-Qa'ida and its affiliates have expressed interest in biological weapons, and issued multiple fatwas and calls for scientists to join their ranks and support their cause.

The FBI remains concerned that certain insiders, especially persons with legitimate admittance to a facility or laboratory working with Select Agents – those organisms we have designated as highly dangerous - could use their access to biological materials and equipment for illicit activities. The FBI continues to assess that many US biological and medical laboratories remain vulnerable to insiders based on several recent incidents involving the illicit acquisition of bacterial and viral cultures. There have been numerous attempts to utilize biological toxins to threaten, injure, or kill individuals. The FBI remains concerned about the availability of these agents for potential criminal use. Additionally, the biological threat is further increased with advances in technologies in the biological sciences that have become more powerful, cheaper, and readily available to much wider audiences.

How the FBI Addresses the Threat

WMDD identifies points of vulnerability in the biological agent exploitation process, and develops countermeasures and prevention initiatives against those points. The process consists of three major activities: acquisition, development, and execution. While the FBI's approach to these activities will not be discussed in detail, this process provides a framework by which WMDD develops and implements its countermeasures, focusing on outreach and tripwire development to address national and regional threat priorities.

Events such as the 1984 Rajneeshee *Salmonella* bioterrorism incident, the Aum Shinrikyo anthrax efforts in the early 1990s, and the 2001 anthrax mailings demonstrate

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01204 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.822

vulnerability to acts of bioterrorism. Due to the unique challenges posed by a bioterrorism incident, such as a covert release which can go undetected for days (until victims seek medical treatment for symptoms), mounting an effective response to an attack requires a high level of cooperation between public health and law enforcement. The lack of mutual awareness and understanding, as well as the absence of established communication procedures, could limit the effectiveness of law enforcement and public health investigations. The effective use of all resources during a bioterrorism incident is critical to ensure an efficient and appropriate response. By working together, public health and law enforcement can achieve their respective objectives of identifying the biological agent, preventing the spread of disease, preventing public panic, and apprehending those responsible.

The FBI and the Centers for Disease Control and Prevention (CDC) developed the Joint Criminal and Epidemiological Investigations training program to improve public health and law enforcement efforts to identify and investigate intentional or naturally occurring threats. The two-day interactive course provides training for law enforcement, public health, and first responders at the local, State, Tribal and Federal level. The focus of this course is on improving local response plans and information sharing protocols, training participants on the joint investigation and interview models, and fostering discussion regarding the local or regional need to develop a Memorandum of Understanding between FBI, law enforcement, and public health on joint investigations.

In addition to being able to identify and investigate intentional or naturally occurring threats, a mission of the WMDD is to promote biosecurity, defined as safeguarding the sources of biological material, persons with experience and expertise, and the technology surrounding the manipulation of the material. Pure sources of biological agents reside in biological supply companies/culture collection entities, research institutions, public health/health care laboratories, and industry. Safeguarding these dangerous biological materials is one key aspect of biosecurity.

Biosecurity, however, is not limited to the security of biological material. It must include the people with the expertise to manipulate, handle, research, and transport biological pathogens and toxins who currently have access to sophisticated equipment and technology related to these materials. Additionally, new areas of research are leveraging other experts, for example computer scientists and mechanical engineers, who have not worked in the traditional framework of biosafety and are unaware of biosecurity matters. Therefore, additional aspects of biosecurity include preventing the persons with the expertise and direct access to the materials from being exploited by outside forces as well as promoting institutional awareness with regard to potential insider-threats.

To address the greater biosecurity issue, the WMDD developed the Biological Sciences and Academic Biosecurity Workshop initiatives to build partnerships between the FBI and the academic research communities, improve situational awareness, and develop a mechanism to report suspicious activities at research entities that could represent an emerging national security threat. These initiatives focus on the vulnerability of terrorist acquisition of biological agents or material housed in research

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01205 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.823

facilities (academic, industrial, private, and clinical), attempts at the exploitation of those with the expertise and/or access to such agents, and the ability of an insider to remove agents of concern for nefarious purposes. The role of the FBI transcends that of a law enforcement/security agency by taking on the responsibility to educate and provide training on security issues, elaborate on the "real world" threat, and act as a resource for mitigating risks. The FBI recognizes that additional stakeholders from Federal, State, and local government and non-government agencies have roles, responsibilities, and resources to ensure safe and secure research with biological pathogens and toxins. Inclusion of these stakeholders and coordinated efforts are also vital for biosecurity.

Entities working with Biological Select Agents and Toxins (BSAT) registered with the Select Agent Program (SAP) are important for national security in two aspects. First, they conduct vital research, from the basic understanding of a biological agent to the development of medical countermeasures against that same agent. This directly benefits the United States' Biodefense architecture. Second, these same entities can be targets of adversaries because of their research. The adversaries may be attempting to illicitly acquire, manufacture, and disseminate biological agents of concern.

The SAP was designed to safeguard those entities that store and/or conduct research with BSAT from adversaries attempting to gain access to the facility, and also to prescribe safety measures preventing accidental release into the environment or exposure of personnel within the facility. This program is a governmental regulation, within 18 USC §175b, regarding the security of BSAT. The SAP, of which the FBI is a Federal partner, is operated by Department of Health and Human Services (HHS) and the United States Department of Agriculture (USDA).

Ensuring that individuals with access to such materials are properly vetted and do not pose a risk as a potential insider threat and/or have the potential for exploitation is of great importance. Each person within the entities is required to undergo a Security Risk Assessment (SRA) prior to gaining access to BSAT. The SRA is processed by the Bioterrorism Risk Assessment Group (BRAG) out of the Criminal Justice Information Services (CJIS) Division of the FBI. The SRA is a database check to determine if the applicant meets any one of ten prohibitors as defined by the USA PATRIOT Act and 18 USC 175b, including being an agent of a foreign power, under indictment for a crime punishable by imprisonment for a term exceeding one year, a fugitive from justice, or an unlawful user of any controlled substance. If a person meets a prohibitor, FBI reports such to the SAP Director and applicant information is referred to the appropriate FBI Field Division for possible investigation. Since the delegation of this responsibility by the Attorney General to the FBI in 2003, BRAG has processed over 35,000 SRA applications. Currently, there are over 13,000 people who are actively involved in the research and/or have access to BSAT.

Both CDC and USDA have compliance and regulatory oversight of all the SAP entities, such as the requirement for periodic inspections of facilities and their inventories. Any accidental release or discrepancy uncovered during inspection is reported to the FBI for further evaluation. The FBI WMDD follows standard protocol of conducting an assessment of the situation to determine if an investigation is required.

Operations

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01206 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.824

The FBI WMD Coordinator (WMDC) is the local point of contact regarding WMD threats and events in each of the FBI's 56 Field Offices. This WMD representative conducts outreach with local biological companies, state and local laboratories, and academia. They also participate in multiple field training and table top exercises that ensure local, State, Tribal and Federal partners are coordinated and prepared for a cohesive response.

The WMDD has a formalized process to assess a potential threat in the field, called the Threat Credibility Evaluation (TCE) process. This allows for discussion and analysis of the situation and involves the WMD Operations Units at FBIHQ, the local WMDC, subject matter experts from the FBI Laboratory Division and relevant local, State, and Federal partners who are directly involved. The TCE process has helped to develop a consistent response protocol and more effectively manage a threat.

Key to addressing the WMD threat is the proper adjudication and analysis of suspected WMD material for traditional forensic evidence. The FBI Laboratory Division is central to the FBI response to WMD crime scenes, secure collection of potentially hazardous materials and the safe examination of evidence. The Laboratory Division provides training to WMDCs, FBI Hazardous Materials Response Teams in the field, local first responders, and Civil Support Teams in regards to the safe, secure and proper handling, collection, and transport of WMD evidence with respect to the inherent hazard and evidentiary value.

The FBI laboratory has developed an extensive protocol and a strong national partnership to deal with all evidence that is contaminated with WMD agents. To identify the presence of biological agents that could be used as weapons, the FBI, CDC, and the Association of Public Health Laboratories established the Laboratory Response Network (LRN). The LRN system provides a local adjudication regarding biological threats associated with items of evidence, before being cleared for entry into the FBI Laboratory where traditional forensic examinations are conducted.

In the event confirming the presence of a biological agent, the investigation process would require prompt traditional forensic examination such as latent prints, DNA analysis, and trace evidence. The FBI Laboratory has taken the lead by developing and implementing the Hazardous Evidence Analysis Team, or HEAT program. The HEAT program provides additional training for qualified forensic examiners and technicians, that allows them to operate in a high-containment laboratory environment such as a biosafety level three or four suite. Qualified forensic examiners conduct analyses of the evidence at one of the FBI's partner laboratories: National Bioforensic Analysis Center (NBFAC), which handles human disease pathogens, and Plum Island Animal Disease Center (PIADC), which handles animal disease pathogens. The FBI recognizes that inherent forensic value can reside within the agents themselves utilized in an attack, and since the 2001 anthrax attacks, the FBI has worked with Federal partners in improving forensic biological attribution capabilities. The Department of Homeland Security (DHS) established the NBFAC and maintains the PIADC, both of which directly support the FBI

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01207 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.825

bioforensic capabilities.

Case Successes

Since the establishment of WMDD, the FBI has successfully managed hundreds of cases involving biological substances and suspicious powders. The following are examples of successes regarding bioterrorism.

In 2006, an adult male collapsed in rural Pennsylvania and was subsequently admitted to a local hospital. Upon completion of blood cultures and secondary confirmatory testing, the patient was determined to have contracted inhalational anthrax. The Pennsylvania Department of Health epidemiologist assigned to the case and the FBI Philadelphia WMDC had both recently attended the FBI-CDC sponsored Criminal and Epidemiological Investigations training. Following the protocol presented at the training, the law enforcement and public health investigators shared their knowledge of the case and collaborated on investigative procedures, including the interviews. The patient was a New York City resident and the artistic director of a West African performance company, who also made and repaired African drums. Following jointly conducted interviews, the patient consented to searches of his home, vehicle, and workspace. Joint environmental sampling was performed by the FBI and CDC, resulting in positive samples in all three locations, with the heaviest contamination in the workspace where the drums were made. The investigation concluded the infection was naturally occurring anthrax related to occupational exposure to contaminated animal skins. Due to the cooperation between law enforcement and public health, this matter and similar incidents have been efficiently addressed through joint efforts.

In 2008, an adult male contacted the Las Vegas Metro Police Department with complaints of difficulty breathing, and was subsequently admitted to the hospital and put under heavy sedation. During a search of the patient's hotel room, police discovered a copy of the *Anarchist Cookbook*, which had been earmarked to a page titled "How to Prepare Ricin," as well as weapons and hand-made silencers. Approximately two weeks later, the patient's cousin traveled to Las Vegas to gather the patient's belongings. The cousin discovered a bag full of what was later determined to be ricin and turned it over to hotel personnel. Hotel personnel notified the police, who contacted the FBI. The patient pled guilty to one count of the Biological Weapons Anti-Terrorism Act (18 USC §175(b)) and was sentenced to 42 months in prison, a $7,500 fine, and three years of supervised release.

In 2008, 65 letters postmarked from Amarillo, Texas and containing an unknown white powder were sent to financial institutions across the US. Some of the letters contained a message stating "Steal tens of thousands of people's money and not expect reprercussions [sic]. It's payback time. What you just breathed in will kill you within 10 days. Thank Mr. Dimon and the FDIC for your demise." In 2009 a subject was charged with one count of false information and hoaxes, and was arrested. During an interview, the subject confessed to the mailings, stating he was motivated by stock losses. He was eventually indicted on 65 total counts and pled guilty to two violations, Threats and False

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01208 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.826

Information, and Threats and Hoaxes (18 USC §1038(a)). He was sentenced to 46 months confinement, a $5,000 fine and $87,734.40 in restitution.

Addressing the Future

Synthetic biology is an emerging field of research which combines elements of different sciences that rely on chemically synthesized DNA to create new biochemical systems or organisms with novel or enhanced characteristics. Advancements in technologies have led to significant progress such as the production of synthetic bacterial genomes and novel methods of pharmaceutical production. The capabilities of these technologies have increased by orders of magnitude over the past few years, and the costs associated with them have decreased by similar orders of magnitude. While these technologies offer amazing promise, they also remain inherently dual-use and just as applicable for nefarious use as reputable use. To that end, the FBI has established the Synthetic Biology/Emergent Biotechnology initiative, which is a proactive approach to mitigate current and over-the-horizon risks posed by the exploitation of advancements in research and development of scientific fields such as synthetic biology and nanobiotechnology. The Synthetic Biology initiative has FBI partnered with synthetic genome providers to render resources and federal reach back capabilities to evaluate uncertainties in customer and/or sequence orders. WMDD is working to develop countermeasures, in partnership with scientific industry and academia to prevent adversaries from acquiring and exploiting material and technology that may pose a national security concern.

Over the past decade, the FBI has witnessed the rapid growth of amateur biology communities. These groups believe advances in science and biotechnology, just like the computer revolution, can be pursued in a home garage or community meeting place and outside of traditional academic and industrial settings. WMDD operates an initiative to develop partnerships with the amateur biology community in order to garner their assistance in preventing, detecting, and responding to incidents of misuse, particularly for nefarious purposes. WMDD efforts focus primarily on outreach and awareness that includes attendance at amateur biology conferences and regional meetings, FBI-sponsored national workshops, assistance in the development of a safety and security framework, and dissemination of education materials. WMDD continues to foster the development of a culture of responsibility and opening lines of communication between members of the amateur biology community and their respective local FBI WMDC to facilitate the reporting of suspicious activity.

Policy

The FBI has taken steps in policy and countermeasure development to address elements of biosecurity, including the security of the biological agents and potential exploitation of persons and technologies, and the bioterrorism threat. The following are highlights of our policy efforts.

The FBI is a member of the Federal Experts Security Advisory Panel (FESAP),

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01209 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.827

created by Executive Order 13546, "Optimizing the Security of Biological Select Agents and Toxins in the United States," which developed recommendations concerning the SAP. As a result, the FESAP was asked to provide consensus recommendations to the Secretaries of HHS and USDA and the Attorney General related to security of the BSAT. Highlighted recommendations include the designation of Tier 1 BSAT (a subset of select agents and toxins deemed to pose the greatest risk), the establishment of appropriate practices to ensure reliability of personnel with access to Tier 1 BSAT at registered facilities, and the establishment of appropriate practices regarding physical and cyber security for facilities that possess Tier 1 BSAT. The Attorney General and Secretaries of HHS and USDA signed a letter with these recommendations to the Deputy National Security Advisor for Homeland Security and Counterterrorism and Assistant to the President.

The FBI developed a Countering Biological Threats Implementation Plan supporting the Office of the President's *National Strategy for Countering Biological Threats*. This plan outlines the FBI's current initiatives in support of the *National Strategy* and the approach for future implementation as applicable within the FBI's roles, responsibilities, and authorities defined in statute or other directives.

WMDD has a detailee within the Executive Office of the President National Security Staff. With a focus on bioterrorism prevention, response, attribution, biosurveillance, and improving global health security, the FBI detailee directly assists the President's principal forum for considering national security and foreign policy matters with senior national security advisors and cabinet officials.

The FBI is a participating member in all biological related policy decisions and is represented at Interagency Policy Committee (IPC) meetings. These IPCs include the Biological Weapons Convention (BWC), BSAT, Synthetic Biology, International Engagement, Biosurveillance and Global Health Security.

As a result of FBI efforts along with the USG and private industry, a DNA screening guidance document was developed, and implemented. This document, the "Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA", was published by HHS in late 2010. This publication represents a milestone, that is, for the first time there is a codified notification process whereby DNA sequence providers are directed to contact their local FBI WMDC upon encountering suspicious customers and/or sequence orders, preventing illicit acquisition of DNA sequences of concern. This is an example of proactive outreach to an emergent field to prevent illicit acquisition of synthetically generated genomic sequences of concern. The FBI will continue to seek partnerships in order to monitor and develop new tripwires and countermeasures as research and development continues at a compounding rate. These partnerships will also help to drive the development of new and effective policy and guidance.

The FBI holds a Federal government *ex officio* position on the National Science Advisory Board for Biosecurity (NSABB), a federal advisory committee within the National Institutes of Health. NSABB was chartered to provide advice, guidance, and leadership regarding biosecurity oversight of dual-use research, defined as biological

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01210 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.828

research with legitimate scientific purpose that may be misused to pose a biological threat to public health and/or national security. The FBI assisted the NSABB in the development of recommendations regarding criteria for identifying dual-use research, principles and tools for the responsible communication of dual-use research, and outreach/education to the scientific community regarding security matters.

The FBI WMDD is a member of the Synthetic Biology Engineering Research Center (SynBERC) Scientific Advisory Board. SynBERC is a multi-institution research effort to lay the foundation for the emerging field of synthetic biology and to catalyze biology as an engineering principle allowing researchers to design, build, and standardize biological systems. As a member of the Scientific Advisory Board, the FBI is in a position to assist SynBERC's activities in addressing ethics and human practices by ensuring biosecurity is incorporated.

Conclusion

Significant progress and partnerships have been made with all levels of government, industry, and the scientific community since the creation of the WMDD; all of which improve the FBI's capabilities in its mission and also support the USG in preventing acts of terrorism on the homeland and US interests abroad. The prevention of bioterrorism requires proactive engagement with the biological sciences community to ensure security is addressed without negatively impacting research progress.

It should be noted the US delegation to the United Nations Biological Weapons Convention (BWC) will be highlighting a range of U.S. activities, including FBI biosecurity initiatives, at the 7th Review Conference in December 2011. By way of background, the BWC was opened for signature in 1972 and entered into force in 1975. It was the first multilateral disarmament treaty banning an entire category of weapons. It effectively prohibits the development, production, acquisition, transfer, retention, stockpiling and use of biological and toxin weapons and is a key element in the international community's efforts to address the proliferation of WMD. One of the key provisions of the Convention is to take any national measures necessary to implement the provisions of the BWC domestically (Article IV). The FBI's mission and activities as described above are in alignment with the Convention, and demonstrate a law enforcement practice and capability not seen anywhere else in the federal government or internationally.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01211 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.829

United States Senate
Committee on Homeland Security and Governmental Affairs

"Ten Years after 9/11 and the Anthrax Attacks: Protecting Against Biological Threats"

Testimony of Thomas Inglesby, MD
Director, Center for Biosecurity of UPMC
October 18, 2011

Mr. Chairman, Senator Collins and members of the committee, thank you for the opportunity to speak to you today on the issue of U.S. preparedness for biological threats 10 years after the anthrax attacks.

My name is Tom Inglesby. I am the Director and CEO of the Center for Biosecurity of the University of Pittsburgh Medical Center (UPMC) and Associate Professor of Medicine at the University of Pittsburgh. The Center for Biosecurity is an independent nonprofit organization of UPMC. Our mission is to strengthen U.S. national security and resilience by reducing dangers posed by epidemics, biothreats, nuclear disasters, and other destabilizing events. Our staff comprises experts in medicine, public health, national security, law, economics, the biological and social sciences, and global health. As you have requested, I will focus my remarks on medical countermeasure development, biosurveillance, and other issues raised in our Center's recent ***Crossroads in Biosecurity*** report on the 10 yr anniversary of the anthrax attacks.

I want to thank this Committee for holding hearings such as today's that focus on protecting the country against biological threats. Pragmatic, informed oversight for challenges of this complexity and importance to national security is essential. In my testimony today, I will include many challenges that we hope will be addressed in the Pandemic and All-Hazards Preparedness Act reauthorization, as well as other biopreparedness priorities.

The potential biological threats to the United States are quite serious. The country could face a new flu pandemic that spreads as efficiently as H1N1 but has case fatality rates like H5N1 or other more lethal strains of flu. It could have to confront a novel virus that jumps from animals to humans, spreads efficiently from person to person, and circles the globe – in the way that the movie *Contagion* recently portrayed.

And the US could have to cope with the use of a biological weapon. The anthrax letters of 2001, tragic and shocking because of the lives lost and people sickened, were only a very small example of a biological weapon. Too many people have taken away from that experience that future bioevents would mirror that one in size and character. While we could see a repeat of the 2001 anthrax letters, biological weapons attacks of the future could be entirely different in character and affect extraordinary numbers of people. In 2009, President Obama's National Security Council said: "The effective dissemination of a lethal biological agent within an unprotected population could place at risk the lives of hundreds of thousands of people. The unmitigated consequences of such an event could overwhelm our public health capabilities, potentially causing an untold number of deaths. The economic cost could exceed $1 trillion for

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01212 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.830

each such incident." Other reports from our intelligence and national security community as well as reports from an independent commission have consistently said that bioweapons are a serious concern, and probably the most likely WMD to be used against the country.

Since 2001, there has been progress in a number of areas of biopreparedness. We have dedicated biodefense programs in many agencies of governments, and many highly effective civil servants in government working on these issues. For example, CDC has made great strides in its state and local public health preparedness programs, its emergency operations planning, its stewardship of the strategic national stockpile, and its management of laboratory security programs. DHS S&T has brought increasing scientific rigor to many of the difficult scientific and technical challenges in bio-response including the Biorisk assessment, the Material Threat Determinations, and their recently completed standards regarding white powder incidents, which are a major advance. The FDA has been working hard to reform regulatory science, to speed its regulatory review process, to seek innovations or alternatives to the Animal Rule, and, to address challenges of making safe and effective products for children. DOD is evolving its Cooperative Threat Mission, working to get more applied science and innovation into its efforts to produce countermeasures, and helping support the international biosurveillance mission. HHS/ASPR has provided grants for hospital preparedness and has continued efforts to develop and procure medical countermeasures. There have also been many important developments at the state and local level, particularly in the realm of better hospital and public health preparedness.

These efforts and programs have helped us make progress against biosecurity threats. And many of the advances over the last decade have also made us better prepared for natural disasters and accidents. In fact, the majority of the work we do to prepare for biological threats will continue to serve secondary purposes that are vital. Our own study of the most recent federal biosecurity budget showed that 92% of funding for biodefense in fact served secondary additional purposes, such as infectious disease research, hospital preparedness and disaster response.

But clearly we are not yet prepared to cope with the biological threats we could face. There are important issues we need to address in countermeasure development, biosurveillance, public health preparedness and more broadly in biosecurity.

Countermeasure development

One of the core, and most challenging, components of our national defense against biological threats is the development and stockpiling of medical countermeasures that can be given to citizens in the event of a biological attack or significant infectious disease outbreak. Development of novel drugs, vaccines, and diagnostics is expensive, inherently a risky undertaking, and is under-funded in relation to the national security need. Large pharmaceutical companies that have experience in advanced development and regulatory processes are not engaged in the development of medical countermeasures for CBRN threats, because there is not a significant enough commercial market for such products, unlike products for chronic diseases and influenza. While some important advances have been made in countermeasure development over the past 10 years, procurement of new products has been limited to countermeasures addressing influenza and a few biological agents.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01213 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.831

In assessing the current status of our countermeasure efforts related to potential bioweapons pathogens, it is important to start with the list of agents identified by the DHS and HHS as presenting the greatest threat to public health. To date, DHS has issued 12 Material Threat Determinations (MTDs) for top priority biological threats to the American public, based on information related to potential public health impact, intelligence and other threat information.

Countermeasures for just three of these threats – anthrax, smallpox, and botulism -- have received the majority of advanced development or procurement funding. Special Reserve Funds have been used to develop and procure anthrax therapeutics and vaccines, a heptavalent botulinum antitoxin, a smallpox vaccine for the immune-compromised, and a smallpox antiviral drug. Although products for some of the other 9 biological threats on the MTD list have received development contracts, they are, by and large, still early in development. The majority of the over 70 products in BARDA's research and development pipeline to counter biological threats are in the early pre-IND or Phase I stage of development. Products in this category of development typically require 8-12 years more of development before licensure, and products at this early stage have a high rate of failure. It is unclear whether new or existing medicines/ vaccines for anthrax, smallpox, and botulism will continue to be the focus over the next 5 years, and/or whether BARDA's focus will be on the procurement of products directed at the other 9 biological agents that are material threats.

Given the number of MTDs and the distance that still must be travelled to develop licensed products for them, it would be quite valuable to understand the roadmap for the process ahead. It would be useful to know the extent to which the development of these needed products requires more basic science versus more advanced development? Clearly the funding for the work should be allocated accordingly. Or for some, specific regulatory problems may be the only remaining issue to address, in which case funding for FDA management of those issues should be the priority. This kind of information is not only critical for planning, but would help all those involved in the MCM development process in and out of government to understand how decisions are being made, and what the priorities of the US government are. It would also illustrate how the process is integrated from its start in basic science to the point when products can be procured.

In addition, when decisions are made to purchase a particular medicine or vaccine for the Strategic National Stockpile, a public explanation should be provided that explains the choice of medicine purchased, justifies the quantities, and explains how that countermeasure will be used operationally in time of crisis. It does not make sense to have products in the Stockpile that cannot be used effectively on the ground in the time of crisis. An added level of explanation will serve to protect the process from undue political influence and will help the public health officials understand the tools at hand and how best to use them in the event of a crisis.

BARDA recently released its Strategic Plan for the 2011-2016 timeframe. In the plan, BARDA says that it has "begun to address the development of broad-spectrum antimicrobials and technologies and platforms with multi-use potential." We support this goal, but want to make sure it does not unduly raise expectations about what is feasible. It is increasingly appreciated how challenging it will be to develop drugs, vaccines, and diagnostic tools that keep pace with the extraordinary advances in biotechnology. As a longer term goal, we should be working to move beyond a one-bug/one-drug approach and aspire to develop and obtain broad spectrum,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01214 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.832

dual use products and platform technologies. Having a portion of the biosecurity R&D effort oriented toward that goal makes sense. However in the near term, there are few scientists or industry leaders who think this kind of shift will happen any time soon, certainly not within 5 years. In the short term (at least the next 5 years) we will need very applied, very directed development of the specific products necessary to address the greatest material threats to the country. There should be transparent and specific goals for product development that are technologically feasible within the 5 year timeframe and are achievable with our current government infrastructure and private sector partners, and prioritized according to the resources available.

It will also be important in the near term to advance ongoing efforts in government to stretch our limited biosecurity resources in smart and sensible ways. For instance, we support government initiatives to, where possible, extend the shelf life of products in the stockpile, investigate the feasibility of reducing the duration of antibiotic courses for prophylaxis, and complete dose-sparing studies that could lead to the ability to vaccinate more people while also decreasing the costs to the government.

My final point on medical countermeasures has to do with funding. There has not been enough advanced development funding in the budget for this process as compared to the funding allocated for basic science. If a private company had committed to developing the full list of required products that the US government is trying to develop, it would have had to commit billions/yr in advanced development funding. BARDA has received a small fraction of that to develop CBRN countermeasures. It is our understanding that the BioShield Special Reserve funds will run out this year. This fund needs to be replenished if we are to continue to procure products for the stockpile.

FDA was appropriately funded to deal with medical countermeasures for the first time last year. But that program's budget was reduced from $170M to $19M in the Senate and $0 in the House in the recent bills. Experts in and out of the government involved in this work widely agree that regulatory challenges are one of the most serious issues to deal with in the development process. Among other things, FDA is responsible for coming up with alternatives or innovations to the Animal Rule and speeding up the review process. This work would be significantly set back or halted altogether if FDA's budget is reduced by 90% or more.

Beyond any one specific program, the changes in the federal budgeting process over the past year have undermined important programs. Within the federal agencies, long-term program planning is nearly impossible when every year is funded via a continuing resolution. New priorities cannot be established, and course corrections are harder to make. How are agency leaders supposed to responsibly manage programs with the constraints of such a system? And how is the private sector supposed to interact with a government that runs like this? The U.S. government should reestablish a clear, sensible, and predictable budget process for biodefense.

Biosurveillance

There has been a good deal of Administration and Congressional attention paid to improving federal, state and local biosurveillance systems, including a major advisory committee to the

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01215 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.833

CDC, a current White House strategy effort and many other initiatives. There have been substantial gains made in biosurveillance, but much work remains to be done.

Biosurveillance systems are seeking to look for evidence of new outbreaks, or they are seeking information to better understand or help contain an outbreak. Information is needed to understand what is happening: how many people are already sick; how is the disease spreading; how severe are the cases; who is most at risk? Other information is needed to understand how an epidemic is unfolding and what public health interventions are working. And other key biosurveillance information is key to the response: which treatments are beneficial; what is the supply of vaccines and medicines; and what medical resources are available. Given the breadth of these information needs and the wide range of organizations that require various elements of this information during different time frames, we believe it is infeasible that any single biosurveillance system can satisfy all of these needs.

In many places, biosurveillance systems are still quite rudimentary, and rely on clinicians and laboratories to phone, fax, or mail in reports of important diseases. If public health officials want to obtain additional information, they often must contact hospitals and clinicians one by one. Each of these time-consuming steps is subject to delay, and it can be difficult to keep up in the midst of a large-scale outbreak. We need to modernize our biosurveillance tools in the following ways.

Electronic Reporting

A major boost for biosurveillance could come from improving public health officials' access to data from healthcare providers, but the ongoing initiative to promote the use of Electronic Health Records (EHRs) across the nation does not adequately address the importance of these data for biosurveillance.

HHS has created a number of criteria for providers to meet in order to receive incentive payments for using EHRs – effectively conveying useful data to public health agencies for biosurveillance purposes is not one of those criteria. In addition, there is no funding for already cash-strapped health departments to allow them to develop data systems to receive incoming EHR data and convert it into actionable biosurveillance information. More than $18 billion in federal funds has been allocated for incentive payments for healthcare providers to promote adoption of EHRs. A very modest portion of these funds should be used to support health departments to enable them to receive and analyze EHR information from providers in order to detect and manage significant outbreaks. If public health continues without this modern capability, then transmission of data from providers to public health offices is almost meaningless.

If you poll many public health officials, they will consistently cite how important electronic laboratory reporting is to their surveillance work. Laboratory information often provides the most precise and reliable information about a new case of illness, and sometimes the earliest information. If an anthrax, plague, or botulism outbreak were to occur, it would be very difficult to get basic information from laboratories that could tell us how many people are infected or how widespread or severe the outbreak is. While electronic lab reporting does occur in some labs,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01216 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.834

particularly in public health labs, it is not uniformly done in the private sector labs which do most of the diagnostic testing overall in the country. Given how important this information is, we need to set a path to ensuring that all notifiable diseases are automatically and immediately reported from the lab to the responsible public health department and continue to be transmitted throughout the course of an outbreak

Diagnostics

Another pressing need in surveillance is the development of technologies to improve the accuracy and speed with which we diagnose sick people. Rapid diagnostics are our best hope for detecting outbreaks early. Although 10 years have elapsed since the anthrax attacks, the diagnosis of this deadly disease is still dependent on assessing a patient's symptoms (which can be imprecise) and/or by growing clinical specimens in the laboratory (which is time-consuming). Rapid, reliable, and cheap diagnostic tests for a range of diseases are within reach, but development is slow, and commercialization is difficult due to high costs, market failures, and other factors. Although U.S. agencies such as BARDA are authorized to develop and purchase the diagnostic tools that will be necessary to manage public health emergencies, progress in this area has been limited. The USG should address this critical gap in our biosurveillance capabilities by making the development and acquisition of diagnostic tools a higher priority.

Data Integration

We also need to do better job combining public health surveillance information with other sources of information that exists in other sectors – such as law enforcement, intelligence or private sector logistical or commercial information. This information resides in federal agencies, state and local agencies and in the private sector. During the 2011 *E. coli* outbreak in Europe and the 2008 Salmonella outbreak in the U.S., it was private sector supply chain and shipping data that proved most useful in identifying the contaminated sources responsible for those foodborne outbreaks. Congress tried to address this problem in 2007 with passage of the "Implementing the Recommendations of the 9/11 Commission" bill, which called on DHS to develop a National Biosurveillance Integration Center (NBIC) to coordinate biosurveillance across the federal government. Though there have been many delays and mis-steps, NBIS has new leadership and has the potential to make real strides on this problem. It would be more effective to work to improve the functioning of NBIS than to give up on the effort. If NBIS does not address it, we will just have to come up with another approach to integration of information.

Public Health Preparedness

In the decade since 2001, many more laboratories have been built and are equipped to test for important diseases. State health departments have hired more epidemiologists to review, investigate, and interpret disease reports, and public health departments are able to maintain 24/7 monitoring capabilities. Prior to the anthrax letters, it was difficult for health departments to detect and conduct surveillance for new viruses, as most lacked even the most basic of surveillance infrastructure and personnel. Preparedness funding greatly strengthened these efforts, so that, for example, when the 2009 H1N1 influenza pandemic was discovered, health departments were able to start performing surveillance for new cases using CDC test kits within

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01217 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.835

days. As health departments have built this capacity to respond to biological threats, they have found these programs quite valuable in preparing for and responding to other disasters.

Recent declines in both federal preparedness funding and state and local financial resources are directly threatening these gains. Federal funding for state and local public health preparedness programs has declined by 27% since 2005 with a cut of more than $100M since FY2010 alone. That loss, combined with state budget cuts due to the economic downturn, has made it difficult for health departments to maintain newly developed information systems and analytical staff.

Significant personnel losses – including trained epidemiologists-- have resulted in reduced capacity, including emergency preparedness capacity, in 40% of public health departments nationwide. There are 44,000 fewer persons working in state and local health departments than there were 2 years ago. There are many examples of the value of CDC funded state and local health department preparedness efforts, not just for biological threats, but for other kinds of responses as well. The Vermont Department of Health (VDH), with the support of CDC preparedness funding and the Career Epidemiology Field Officer program, has been critical in responding to the release of radioactive materials at the Vermont Yankee nuclear power station this year. In response to devastating flooding in the Midwest, the North Dakota Department of Health assisted in the evacuation of thousands of citizens and led the evacuation of hundreds from vulnerable healthcare facilities. The department pre-deployed medical sheltering for up to 700 evacuated patients and mobilized medical volunteers. In 2008, Kentucky received over 1,500 evacuees from Hurricane Gustav who were victims from the coast, and the Kentucky Department for Public Health supported the medical needs of evacuees. The New Jersey Department of Public Health responded in 2011 to one of the most devastating natural disasters to impact the state, Hurricane Irene, working double and triple shifts to provide care to the more than 3,500 evacuees and victims, including those from over 40 healthcare facilities.

If the proposed cuts take place in this year's CDC preparedness budget, preparedness efforts like those will be threatened. As many as 1,500 front-line state and local public health professionals would need to be eliminated. The cuts would degrade national capability for disease detection, monitoring, and real-time situation awareness -- this capability was essential in responding to H1N1.

The cuts would also eliminate CDC's ability to prepare for nuclear or radiological terrorism, to include assisting state/local health departments with radiological exposure, contamination assessments, field investigations and advice on protective actions related to direct/indirect human and animal exposures. They would diminish the capacity of CDC's diagnostic program for emerging diseases; the chemical laboratory and response programs; the Epidemiology and Response Branch; and, the Laboratory Response Network. And the cuts would eliminate all funding for the academic Centers for Public Health Preparedness which is the only CDC external funding for academic research that focuses on improving preparedness. For all these reasons, I would urge Congress to reverse these cuts to CDC funding.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01218 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.836

Additional priorities

Hospital preparedness

Prior to 2001, there were few dedicated hospital preparedness efforts. Preparing hospitals to respond to disasters was often a vocational after-hours pursuit. The preparedness standards of the Joint Commission (the entity that accredits most U.S. hospitals) were minimal at the time and there was very little in the way of federal or state guidance or funding. Following the 9/11 attacks and the anthrax letters, hospital preparedness greatly improved due in large part to the Hospital Preparedness Program (HPP) in HHS/ASPR and the upgrading of the Joint Commission's preparedness standards.

My colleagues at the Center documented this improvement in a nationwide study published in 2009. We found that in addition to significant improvement in preparedness of individual hospitals, collaboration among hospitals and between hospitals and local and state government agencies had greatly improved. We found that in many locations, hospitals and agencies had created formal or informal coalitions to address healthcare preparedness and response. The benefit of these coalitions has been demonstrated in a number of recent events, including the Virginia Tech mass shooting, the Minnesota bridge collapse and the 2009 H1N1 influenza pandemic.

Although preparedness has improved at most hospitals in ways that should improve resilience to more common disasters, such as tornados, multiple victim shootings, fires, etc, we found progress limited in efforts to prepare for catastrophic health events— a disaster that would result in many thousands of patients. Examples of such an event would include wide-area bioterrorism, a nuclear detonation and a large earthquake. Neither hospitals, local jurisdictions, states nor the federal government have realistic plans for how the medical needs of this many people could be adequately addressed.

The federal National Disaster Medical System (NDMS), which has been valuable in responding to many crises, would have limited capacity to respond to the events of a catastrophic health event. Collectively, all of the deployable medical resources of NDMS would be insufficient for the response. Many patients would need to be transported to private hospitals around the country. NDMS has contracts with thousand of hospitals for this purpose and depends primarily on the U.S. Air Force to transport patients over long distances. However, the military's capacity to move patients is limited and takes considerable time to ramp up. There is not currently a feasible plan regarding how to move large numbers of patients to other areas of the country for care. The role and capacity of NDMS in such a catastrophe should be reexamined, including its deployable teams, its transportation capacity and its definitive care (hospital) component. In addition, HHS will need greater involvement of the private sector to enable an effective response on this scale.

Decontamination

In 2001, government buildings and media offices contaminated by anthrax spores were remediated to the highest possible standard—to the point at which zero viable anthrax spores

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01219 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.837

could be detected. The process was thorough but costly and slow. It would be impossible to replicate following a wide-area attack.

Because there are few historical examples of aerosolized releases, we have limited information regarding the level of infectivity and aerosol dynamics of anthrax spores deposited on surfaces. We don't know how likely *B. anthracis* spores are to cause disease in humans after re-suspension, and we do know the probability of re-suspension can differ depending on surface (i.e., concrete, carpet, vegetation, etc.) and climate. Health risk is especially uncertain when it comes to outdoor environments. We need to know if the 2001 standard of zero viable spores is necessary, or if there is a less rigid standard that is reasonable and acceptable. There are some research efforts underway to examine these issues, and these should be supported and encouraged.

In addition to scientific research, there are a number of things that the federal government can do to improve our remediation capabilities. We need to ensure sufficient laboratory resources - remediation after an anthrax attack will begin and end in the laboratory. The necessary labs must have the resources and capabilities to deal with this kind of event.

Conclusions

The country has made steady progress in the last decade, but there is much more that needs to be done to make us resilient to biological threats. There is vitally important work to do in countermeasure development, public health preparedness, biosurveillance and other key issues in the years ahead. We hope that the coming reauthorization of the Pandemic and All-Hazards Preparedness Act will address many of the issues that I have outlined today. Thank you for this opportunity to provide recommendations in each of these areas.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01220 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.838

WRITTEN TESTIMONY OF DR. ROBERT P. KADLEC
U.S. SENATE HOMELAND SECURITY & GOVERNMENT AFFAIRS COMMITTEE
October 19, 2011

Chairman Lieberman, Senator Collins and Members of the Senate Homeland Security and Government Affairs Committee; it is both a privilege and opportunity to appear before you today. As one of three individuals who served as Special Assistant to the President for Biodefense Policy under former President George W. Bush, the opportunity to convey some insights, lessons learned and opportunities for improvement on the occasion of 10th anniversary of the anthrax letter attacks is one I welcome and appreciate.

Since the fateful events of the Fall of 2001, much has been done and progress has been made in our preparation for potential deliberate biological attacks and natural pandemics. This is credit to three consecutive administrations beginning with President Bill Clinton, President George W Bush and continuing with President Barak Obama and important contributions made by legislative branch.

It is important to underscore the role of Congress in setting and enabling policies by passing biodefense related legislation beginning with the Public Health Preparedness Act in 1998. Congress has appropriated approximately $65 B in the last 10 years creating and sustaining state and local emergency service and public health preparedness capabilities, funding research, development and procurement of medical countermeasures, improving hospital and first responder preparedness.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01221 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.839

Progress has been made though it has suffered through fits and starts. While much has been done, we are far from being adequately prepared.

Senators Bob Graham and Jim Talent of the WMD Center released their "Bio-response Report Card" last week. Your former colleagues made an invaluable contribution to this subject by providing a timely assessment of the progress, shortcomings and persistent vulnerabilities posed by a range of potential biological risks. Specifically, they noted that while the U.S. could potentially handle small-scale event like that experienced in 2001; we are not prepared to deal with a large scale event that Al Qaeda has reportedly intended to conduct.

I also note the recent testimony and public statements by the former National Counterterrorism Center Director Michael Leiter indicating his concern about the risk from chemical and biological terrorism. As he said in during the Aspen Security Forum in July 2011: "The potential threat from al-Qaida in the Arabian Peninsula is very real. The most likely...are simple forms of chemical or biological weapons (rather than a nuclear attack). Is it going to kill many people? No. Is it going to scare people? Yes."

The difficulty in discriminating between a “small” event and a “large event” is relative. As the current Food and Drug Administrator, Dr. Margaret Hamburg stated in 2006 had the perpetrator of the 2001 anthrax letter attacks released the contents of one anthrax laden envelope in the ventilation system of the World Trade Center more people could have died than from the airplane attacks. Doing the same in the air shaft of the New York Subway system where several million people ride daily may only kill a relatively few but scare millions to seek preventive antibiotic treatment and contaminate a vital major transportation hub.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01222 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.840

The grades issued by the WMD Center indicate that there are a of number preparedness areas where the US Government has improved, and others which have faltered and in some cases failed to make substantive progress. While their assessment is a snapshot in time, it highlights a number of preparedness areas that have chronically lagged:

- Rapidly detecting environmental releases of biological agents and diagnosing pre-symptomatic and early clinical disease from the top biological threats such as anthrax.
- Developing and procuring medical countermeasures such as preventive vaccines and therapeutic drugs against the top threats.
- Rapidly dispensing the antibiotics and vaccines that we already have in the Strategic National Stockpile.
- Rapidly assessing and decontaminating areas where anthrax has been released.

These are just a few critical areas where progress has been little, slow or halting. These are obvious areas where it is vital to make improvements.

Issuing grades are illustrative and helpful to assess where we stand. But, they are frankly abstract to the grim reality they represent. Failing grades are a surrogate for the potential consequence that Americans may die, in large numbers, unnecessarily in the event of an attack. An "F" is a simple way of saying that the Government is derelict in its duty to adequately organize, train or equip responders nor enabled the public to prepare themselves for this kind of risk.

There are two major obstacles to overcome in our efforts to be better prepared for this risk. The first is our understanding of the true nature of bioterrorism and biowarfare. One of the major

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01223 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.841

current misconceptions is to conflate natural threats like pandemics and deliberate threats from terrorism or acts of war by nation states. I do not challenge the notion that Mother Nature can inflict significant loss of life, economic and social disruption through natural evolution of emerging diseases. The 1918 Spanish Flu and more recently SARs are two vivid examples. Such a scenario is the subject of the popular current movie "Contagion" that depicts the challenges and potential consequences of an emerging highly infectious and virulent Nipah virus. Some equate the natural threat to what a terrorist or nation state is capable of doing deliberately.

I strongly reject this notion and wish to point out the fallacy of this thinking. We do the nation a great disservice if we perpetuate the assumption that the deliberate biological threat from potential adversaries is a lesser included case of influenza for example.

Mother Nature is not a thinking enemy who intends to inflict grievous harm to our country, to kill our citizens, undermined our government and destroy our way of life. The risk of conflating natural and deliberate biological events is failing to appreciate the relevance of Clausewitz and the principles of biowarfare that include:

- Developing highly virulent organisms that are likely resistant to our current stockpiles of antibiotics;
- Disseminating very high doses of infectious agents that may be a combination of more than one agent that result in more rapid onset and more virulent than seen in nature;
- If disseminated effectively, result in lethal equivalence to nuclear weapons
- Targeting not necessarily our military forces but our civilian population which represents our willingness to protect our national interests.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01224 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.842

These principles are not new but were learned and noted in 1969 as a result of the cumulative experience of our former offensive biological weapons program. Simply preparing for deliberate threats as a subset of or equivalent to natural events is not only wrong but dangerous.

The second is the special and extraordinary role of the Federal Government in confronting the risk from deliberate biological threats. One of explicit and implicit assumptions of homeland security has been "All disasters are local." This is reasonable and appropriate in other disaster scenarios. The practical manifestation of this assumption has been focusing Federal investments and efforts in improving State and local preparedness. As all disasters start locally, the responses begin locally. But deliberate biological events should be viewed as attacks on the nation. The Constitution indicates that our Federal Government has the principle responsibility for the common defense.

It may be impossible to immediately determine the perpetrator as a nation state, terrorist group, deranged individual or Mother Nature but the consequences can be profound socially, economically and politically. Though an attack may be local, its consequences will be felt nationally and internationally.

There is a growing appreciation that there is an increased role for the Federal Government to directly assist State and local authorities in the event of a biological attack. President Obama signed an Executive Order in December 2009 specifying a greater role for Federal Departments and Agencies such as the US Postal Service and the Department of Defense to dispense medical countermeasures for example.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01225 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.843

But the Federal Government has yet been fully mobilized to this task and has yet to determine and commit the other capabilities needed to respond to a large scale attack. It is not only unfair but foolhardy to expect that State and local authorities could effectively respond without significant Federal public health, medical, security, transportation and recovery and remediation support.

An analogy of the current situation may prove helpful. Following 9-11, the Federal Government placed the majority of the burden on State and local authorities, particularly public health, to deal with the deliberate biological threat. As you appreciate, it is a complex national security threat. It would be somewhat similar to telling Mayor Bloomberg after the 2001 World Trade Center airplane attacks that he would bear the responsible for detecting and defending against similar attacks in the future. New York does not have the wherewithal to do so. Similarly, they and other major cities do not have the means to respond to a large scale biological attack.

While I identified a number of areas of critical deficiencies and near term opportunities for improvement, I am going to focus one particular area highlighted by the Graham Talent Report Card—leadership. They identify it as the first of their three strategic priorities. I firmly believe that leadership is currently the critical missing ingredient and is the "secret sauce" to progress and future success.

Without strong leadership that emanates from the White House that is propagated through the Federal Departments to the state and local authorities, no amount of money will make us sufficiently prepared.

This Administration has demonstrated such leadership on the threat from nuclear proliferation. The President has been front

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01226 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.844

and center and has made the cause of nuclear non-proliferation and nuclear arms reduction a centerpiece of his policies. He has rallied the Executive Branch, Congress and the International Community to the threat from nuclear weapons. It is troubling to see the lack of similar commitment to this issue. And without the President's visible concern or commitment, the best efforts of some in his administration will be ineffective. White House involvement is essential to ensure that certain departments and agencies live up to their interagency obligations under the national response framework and the Emergency Support Functions particularly the Departments of Homeland Security, Health and Human Services, Defense, Veterans Affairs, Justice and the Environmental Protection Agency. Each agency has explicit responsibilities and critical capabilities to bring to bear. Ensuring the effective coordination of preparedness activities and execution of response efforts is critical to ensure that American lives won't be lost needlessly.

Visible leadership is not only a requisite for the Executive Branch. Congress too has a vital leadership role. In lieu of concerted efforts by the Administration, Congress can effectively advance preparedness. There is homeland security legislation currently being considered in the Senate within this Committee and within the Health Education Labor and Pension Committee reauthorizing the Pandemic All-Hazards Act. There are bills in the House Homeland Security and Government Affairs and Energy and Commerce Committees. Hopefully, Congress will act to pass one or ideally both bills before the end of this session.

In addition to specific legislative initiatives, the power of oversight being demonstrated here today is an important adjunct to ensure that responsible Federal authorities are meeting their obligations. In these difficult fiscal times, it is hard to ask necessarily for more money but it is vital to preserve what funding has been allocated to this risk.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01227 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.845

To provide some basis of comparison, the U.S Government spends close to $15 B annually on nuclear defense and 17 $B on cyber-warfare defense and nearly $7 B on biodefense. An analysis by the Council of Economic Advisors during the Bush Administration calculated the short term economic impact of a single large scale anthrax attack that could kill several hundred thousand people in a major metropolitan area at approximately $1.5 Trillion dollars. Small targeted increases in funding to sustain State and Local emergency services and public health and improve medical countermeasure advanced development and dispensing would be two worthy candidates for consideration.

I thank you Chairman Lieberman and Senator Collins for this opportunity and look forward to your questions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01228 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.846

Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats
Testimony of Jeffrey Levi, PhD
Executive Director, Trust for America's Health
Senate Committee on Homeland Security and Government Affairs
October 18, 2011

Chairman Lieberman, Ranking Member Collins, and members of the Committee: my name is Jeff Levi, and I am Executive Director of Trust for America's Health (TFAH), a nonprofit, nonpartisan organization dedicated to saving lives by protecting the health of every community and working to make disease prevention a national priority. I am grateful for the opportunity to testify before the Committee on the progress and challenges we face on the 10 year anniversary of the anthrax attacks on our nation.

A decade ago, public health was on the frontlines of our battle for national security. From the moment an infectious disease physician first contacted his local health officer in Palm Beach County, Florida about a possible case of inhalational anthrax, public health had to face the unimaginable. Today, we know we need to expect the unexpected. Public health's role is crucial in emergency preparedness and response: health departments perform the surveillance that detects the first few cases of an outbreak or attack, laboratories test the samples, epidemiologists conduct the investigation and pinpoint the source, and public health workers coordinate the medical response, advise and communicate to the population, and distribute vaccines or drugs that help save lives. Over the last decade, we have made dramatic progress in meeting this responsibility. But unfortunately, as I outline in my testimony, that progress is greatly threatened by recent funding cutbacks at the federal, state, and local level and we could face the sad irony that if another anthrax attack were to occur today, we may be better prepared than 10 years ago – but possibly not as well as three years ago.

Public Health: Where We Were in 2001

Last month, TFAH and the Robert Wood Johnson Foundation released a new report, *Remembering 9/11 and Anthrax: Public Health's Vital Role in National Defense*, which features more than 30 firsthand accounts from national, state, and local leaders who were on the ground in response to these dual tragedies. In developing this report, we learned that the public health system mounted an extraordinary response to these events despite limited familiarity with bioterrorism and decades of underfunding that left it with a deficit in technology, workforce, and training. For example, in Connecticut, where the last victim of anthrax died, the Naugatuck Valley health department unearthed municipal response plans that dated back to World War II and the Cold War.

Among the challenges the public health system faced in 2001, as noted by contributors to our report, were:

- There was not a clear public health response system in place for handling unexpected emergencies, so much of the response was developed on the fly;

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01229 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.847

- There was little to no experience in infectious disease countermeasures research and development;
- Hospitals treating anthrax victims had received limited guidance on how to manage a bioterrorist event before victims started presenting;
- Many health departments lacked internet, blast fax, computers, and the ability to receive and respond to urgent case reports 24/7, so communication among CDC, public health, and healthcare providers often did not happen in real time;
- Biosafety Level 3 laboratory space was not a standard feature in state public health labs, as it is today, so many labs did not have the equipment and procedures to properly secure evidence for storage;
- CDC and state and local health departments faced a crushing demand for information and recommendations, and CDC had not yet adopted the incident command system.

Despite these challenges, as we know, public health rose to the occasion. The Laboratory Response Network, which is now an integral piece of the BioWatch program, tested 350,000 environmental samples and clinical specimens over an extended period. CDC provided national surveillance, laboratory diagnostic support, treatment recommendations and advice on postexposure prophylaxis. And public health helped to calm a nation by putting science first in risk communications, rather than allowing the public to succumb to speculation and hysteria.

A Decade of Gains

There were significant investments in public health preparedness and infrastructure immediately after 9/11 and anthrax. In June 2002, Congress passed the Public Health Security and Bioterrorism Response Act, which established cooperative agreement funding support for state health departments around the country. In 2006, Congress reauthorized the legislation as the Pandemic and All-Hazards Preparedness Act (PAHPA). Congress has also appropriated billions of dollars through Project BioShield and the Biomedical Advanced Research and Development Authority (BARDA) to invest in vaccine research and development.

Since FY 2003, Congress has since invested over $12 billion in state and local public health preparedness, hospital preparedness, and pandemic capacity at the state and local level.[1] This outlay has led to tremendous progress in our ability to prepare for and respond to an emergency. Our report highlighted some of these accomplishments:

- All 50 states now have pandemic flu plans, compared to 13 states in 2003;
- All 50 states have adequate plans to receive and distribute supplies from the Strategic National Stockpile, up from 2 states in 2003;
- 49 states increased or maintained Laboratory Response Network chemical capacity in 2010; compared to 10 states in 2005;
- 75 percent of hospitals participating in the Hospital Preparedness Program (HPP) met 90 percent of programmatic goals; and

[1] Sources: Trust for America's Health, *Ready or Not? 2010: Protecting the Public's Health from Diseases, Disasters, and Bioterrorism*, p. 36. Dec 2010: http://healthyamericans.org/reports/bioterror10/; CDC Fiscal Year 2011 Operating Plan: http://www.hhs.gov/asfr/ob/docbudget/2011operatingplan_cdc.pdf; Public Health and Social Services Emergency Fund Fiscal Year 2011 Operating Plan: http://www.hhs.gov/asfr/ob/docbudget/2011operatingplan_phssef.pdf

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01230 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.848

- BARDA and Project BioShield have made critical investments in domestic medical countermeausure research and development and procurement, including the first contract for a cell-based flu vaccine, expected in 2014.

And public health preparedness has made leaps and bounds in less tangible ways.

- Now, we recognize that bioterrorism and emergency preparedness are as integral to the role of public health as disease prevention and health promotion. We have fully developed the rapid response capabilities so that health impacts are considered and mitigated from day one of an emergency. During the Gulf Oil Spill, for example, the Louisiana Department of Health and Hospitals immediately began conducting testing and surveillance to monitor the possible effects from oil and dispersants on human health, water quality, and seafood safety; providing mental health services; and providing risk communications to the public.[2]
- Public health also has a much stronger relationship with the emergency response, public safety, and health delivery systems. This coordination has been spurred along by federal grant programs and by planning processes such as development of pandemic flu response plans.
- Health departments and the CDC now have substantial experience with crisis risk communications and are employing multiple technologies to get crisis messages to the public and media. These skills are critical when competing with misinformation and paranoia that can accompany a public health crisis.
- We have also made tremendous strides in situational awareness, or the ability to gather relevant information during an event, analyze it, and take appropriate action. Public health is more accustomed to the incident command system structure. For example, during the H1N1 flu outbreak, CDC, in partnership with state and local health agencies, provided real-time daily data for flu surveillance ahead of the second wave.

Challenges and Opportunities

This progress is a result of a significant investment by the federal government. Unfortunately, these improvements cannot be maintained with one-time investments. Training of our public health workforce must be ongoing; vaccines and antivirals in the Strategic National Stockpile are expiring or have been used, as during the H1N1 pandemic, and not necessarily replenished; technology is quickly becoming outdated; and health departments need predictable funding to operate laboratories, respond to emergencies, and investigate outbreaks. And yet, federal support for public health preparedness has been cut by 37 percent, adjusting for inflation, since FY2005. These cuts are a particular concern because most local health departments, as well as many state health departments, depend on federal funding for most, if not all, of their public health preparedness funding. As a result, I worry deeply – as do my colleagues on the front lines of public health agencies – that our capacity to respond to a new emergency will be severely diminished in the near future.

Moreover, the cuts at the federal level have been matched or exceeded at the state and local level as state and local spending has been slashed in response to the recession and its aftermath. In

[2] Louisiana Department of Health and Hospitals, "Oil Spill Response Efforts," Presentation to Louisiana House of Representatives, June 9 2010: http://www.dhh.state.la.us/offices/publications/pubs-378/Oil%20spill%20presentation_06092010.pdf

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01231 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.849

fact, 33 states cut funding for public health from fiscal year 2008-2009 to 2009-2010, and 18 of these states cut funding for a second year in a row. We fully expect that the data for 2011 will be far more grim. While, as I noted, most preparedness funding comes from the federal level – the federal investment assumes and builds on a core capacity at the state and local level. That is fast eroding, undermining the foundation needed for the federal preparedness investment.

These budget cuts are not just about money to purchase supplies and equipment. They are about the people who are essential to an effective public health response. Today, we also face a workforce crisis. Were a major public health emergency to occur today – even compared to the demands of the pandemic H1N1 just two years ago – there might not be enough workers to effectively respond and certainly fewer than just a few years ago. According to the Association of State and Territorial Health Officials (ASTHO) and the National Association of County and City Health Officials (NACCHO), 44,000 state and local public health positions were lost between 2008-2010 as a result of budget cuts.[3] While we may be able to quickly order supplies in reaction to an event, we simply cannot quickly hire and train a 21st century public health emergency workforce *after* an attack occurs. The investments made through CDC's Public Health Emergency Preparedness (PHEP) grants have provided our health departments and laboratories with the staff, training, planning, and exercises needed to rapidly respond to a disaster. Several contributors to our report note that the anthrax and 9/11 attacks marked the beginnings of relationship building between the public health, health care delivery, and traditional homeland security and first responder communities. As we lose these positions by the thousands, so too do we lose the trust and communication occurring on the ground in every community.

We're also facing barriers in our health care system's capacity to care for a massive influx of patients. Although we've made progress in hospitals' planning and preparedness for a disaster, there is still a lack in preparation for a catastrophic health event. We believe, rather than individual hospital preparedness, we should be thinking more broadly about health system preparedness. Since initiatives such as the HPP do not have the funding to bring every hospital up to a basic level of preparedness, we are encouraged that HHS is starting to think strategically about Healthcare Coalitions, which promote regional collaboration and networking among hospitals and public health. We hope that this initiative expands nationwide and broadens to include the entire the healthcare delivery system. Yet, uncertainty remains about how the health system would respond to a catastrophic health event today: how we would allocate limited life-saving resources, the liability, legalities and ethics of providing care, and delivering medical countermeasures to large numbers of people.

We have been pleased to see progress in the research and development of medical countermeasures in the past five years, but the nation is still falling behind. For example, our significant investments in vaccine development allowed production of an H1N1 vaccine in record time, but manufacturers were only able to produce limited quantities by the beginning of the second wave of the H1N1 pandemic because of limited capacity and reliance on an outdated egg-based production method. The Administration and Congress need to prioritize investment in development of medicines used during a public health emergency, as the limited commercial

[3] Association of State and Territorial Health Officials, "Budget Cuts Continue to Affect the Health of Americans: Update May 2011." http://www.astho.org/Display/AssetDisplay.aspx?id=6024

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01232 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.850

viability of such products demands government intervention. The Pandemic and All-Hazards Preparedness reauthorization bill, currently being developed by the Senate HELP Committee, should include reauthorization of Project BioShield, significant investment in the Biomedical Advanced Research and Development Authority (BARDA), and authorization of a Medical Countermeasure Strategic Investor firm to leverage private and public capital and provide management support to biotech companies. These kinds of investments have dual benefits of building America's readiness for outbreaks as well as developing the biotech workforce. We would also like to see Congress support FDA's nascent regulatory science program, which seeks to build the science base at the agency necessary to oversee development and approval of drugs for new and reemerging threats. We applaud the goals of the review of the federal medical countermeasure enterprise and BARDA's five year strategic plan, the latter of which includes goals to build US manufacturing infrastructure, flexible manufacturing, and the capability to rapidly develop medical countermeasures during a public health emergency. We hope Congress provides the resources and legislative authorities to realize these goals.

Finally, there are challenges and opportunities in the way our nation approaches biosurveillance. Remaining constantly aware of surrounding threats and our capacity to respond are critical to dealing with emergencies. Our disease surveillance system has been built one disease or crisis at a time, resulting in archaic and static silos of information rather than as an interoperable system with a focus on prevention. We need to fundamentally rethink how we do biosurveillance – for both emergencies and routine public health issues. The particular challenge in the field of preparedness is that we don't necessarily know in advance what we will need to know, and thus the most comprehensive approach to data collection is needed. Our fragmented system of data reporting drastically weakens our nation's defense against emergency outbreaks.

We must harness the opportunities afforded by the nation's transition to an integrated health information technology (HIT) system with electronic health records at the core. This could create economies of scale and provide more useful information to public health and national security officials. We understand that the White House is currently examining our national biosurveillance system. We believe there needs to be a new national strategy that examines means to achieve interoperability, efficiency, and transparency among various surveillance systems in order to create an integrated biosurveillance operation. In particular, we must strengthen HIT meaningful use requirements, which currently contain weak public health reporting requirements. We have begun building the capacity of health departments to receive this data through grants from the Recovery Act and Prevention and Public Health Fund, but these investments need to continue and grow. We also urge ongoing, enhanced communication between Congress, CDC and the Office of the National Coordinator for Health IT (ONC) to ensure that ONC considers the preparedness implications of EHRs.

Conclusion

Our report finds that the United States often takes a band-aid approach to public health preparedness, i.e., as new emergencies and concerns emerge and attention shifts, resources are diverted from one pressing priority to another, leaving other ongoing areas unaddressed. In our report, NIAID Director Anthony Fauci writes:

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01233 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.851

> *"The biggest threat to bioterrorism preparedness today is complacency. If a health threat does not happen, be it naturally occurring or deliberate, we tend to make it a lower priority. The worst thing we can do is to make something a priority after it happens. After it happens is too late; you are playing catch-up. Preparedness for a threat must be a priority before it happens."*

Numerous contributors to our report echoed this sentiment. I am encouraged to see this Committee is taking these threats seriously. Thank you again for the opportunity to be here today, and I look forward to your questions.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01234 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.852

Post-Hearing Questions for the Record
Submitted to the Honorable Alexander G. Garza
From Senator Mark L. Pryor

"Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats"
October 18, 2011

Question#:	1
Topic:	exposure
Hearing:	Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats
Primary:	The Honorable Mark L. Pryor
Committee:	HOMELAND SECURITY (SENATE)

Question: What is Office of Health Affairs doing to address rural communities in which biochemical exposure might not create a mass casualty incident as quickly as would occur in an urban area, but would nevertheless result in higher casualty numbers due to lack of access to treatment? How have you worked with rural communities to address the issue of biochemical preparation and containment?

Response: The Office of Health Affairs (OHA) remains focused on promoting local public health preparedness for human, animal and agricultural diseases in all communities. OHA partners with other agencies to provide technical and logistical support to Federal preparedness initiatives, and it works closely with the Department of Health and Human Services, which has primary responsibility for federal medical and public health response to emergency events. OHA recognizes that local public health, emergency management, and law enforcement communities have an integral role in addressing biological and chemical exposures in local communities, to include rural areas. OHA is working to develop standardized protocols for DHS emergency medical services (EMS) personnel who provide medical care, force health protection, disaster response, and search and rescue in remote and medically austere locations, where local emergency medical services do not operate. These services are primarily for DHS employees and those in need of immediate life-saving medical care. In addition, OHA helps in the department-wide coordination of preparedness grants that have a health and medical nexus, and is currently developing additional technical guidance and tools to support State and local communities' capabilities development. This guidance is designed to help State and local communities bolster efforts to prepare for and respond to catastrophic health threats.

67123.853

Dr. Nicole Lurie, Assistant Secretary for Preparedness and Response
Department of Health and Human Services
HSGAC Questions for the Record
October 18, 2011 Hearing
"Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats"

From Senator Mark L. Pryor

1. In 2007, in response to questions submitted for the record, HHS told this Committee that our national stockpile of the anthrax vaccine was produced inside the United States. Is that still the case?

Yes, BioThrax, also known as Anthrax Vaccine Adsorbed (AVA), is produced and licensed for pre-event usage in the United States.

a. **Based on the threat today, are we producing more or less of the vaccine?**

Since the first Project BioShield (PBS) procurement contract awarded in 2005, Emergent has maintained production capacity at approximately 6-7 million doses per year. In 2010, BARDA awarded a contract to Emergent to facilitate expansion of domestic anthrax vaccine manufacturing capacity from a new and larger facility. Expectations are that Emergent will be able to manufacture approximately 26 million doses per year later this decade.

b. **Do the manufacturing companies have the ability to meet the demand in the event of an anthrax incident that spans many states or even the nation?**

The current HHS requirement is to protect 25 million Americans after an anthrax attack. Based on the concepts of operations, individuals would receive three doses of vaccine (Post-exposure-prophylaxis (PEP) regimen) concurrent with 60 days of antibiotics. The current vaccine has a 4 year expiry. Thus, Emergent cannot produce enough vaccine in their current facility to meet the HHS requirement.

HHS has taken a multi-prong approach to resolve this disparity. First, as mentioned above, the BioThrax anthrax vaccine is licensed as manufactured in the current Emergent facility, but it is now necessary to produce it in the new Emergent vaccine manufacturing facility and, thus, necessary to license it as produced there; BARDA supports the validation and clinical studies that would be the basis for that license. Second, BARDA supports the advanced development of four (4) next generation anthrax vaccine candidates based on recombinant protective antigen (rPA). Lastly, studies are underway by HHS agencies, including NIAID, CDC, FDA, and BARDA to investigate the possibility of stretching the licensed anthrax vaccine stockpile in the event of an emergency where the need is greater than the available vaccine.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01236 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.854

Dr. Lurie, ASPR
QFRs
HSGAC Hearing October 18, 2011

2. **What steps has HHS taken to secure a diversity of products in the strategic national stockpile from various manufacturers in order to avoid a single point of failure with the anthrax vaccine?**

In addition to supporting the existing BioThrax vaccine from Emergent, HHS supports the development of next generation anthrax vaccines. BARDA supports the advanced development of four (4) next generation anthrax vaccine candidates based on recombinant protective antigen (rPA). Three next generation vaccine candidates (Emergent, Pfenex, and PharmAthene) express the rPA protein in different bacterial expression systems and all are administered intramuscularly, while a fourth candidate (Vaxin) is administered intranasally using an adenovirus-based vector system. Furthermore, BARDA and NIAID are supporting studies using both the licensed AVA and rPA vaccine candidates using new adjuvants (e.g., CpG) that may provide greater immunity with fewer doses and less antigen per dose.

From Senator Scott P. Brown

1. **My understanding is that HHS entered into a sole source contract for 44.7 million doses of an anthrax vaccine developed in the 1950s. Is it true that, according to a Center for American Progress Report released last year, the Federal Government is paying almost a 300 percent markup on every dose of this vaccine even after paying for the entire cost of developing this vaccine?**

The Government paid fair market compensation for Anthrax Vaccine Adsorbed (AVA) doses delivered. The pricing to the government was substantially below market price. The price paid was based on an Independent Government Cost estimate and independent negotiations with both DoD and HHS. In each case, the Contractor was required to provide and prepare price justification (certified) prior to the award. The 300% calculated profit is erroneous because there are many factors other than cost of manufacture that contribute to the pricing of biodefense countermeasures, e.g., cost of maintaining an FDA-compliant facility. The final cost is $400 million less than the manufacturer's initial proposal, and represents a savings of more than $64 million relative to the per dose price paid in the previous contract.

2. **Do you believe that this is the best use of tax payer dollars?**

Yes. The Government negotiated diligently to obtain the best price and best value for a product that will help protect the public health and national security.

3. **Last week, Tom Ridge, former Secretary of DHS, commented about a recent contract "for a billion plus for the first generation" anthrax vaccine, when there was a 2004 requirement for a second generation vaccine. Can you confirm that $2.6 billion in contracts have been awarded for this older vaccine?**

In the absence of a next generation anthrax vaccine in late stage development, the federal government has procured BioThrax, also known as Anthrax Vaccine Adsorbed (AVA), which is licensed in the United States to prevent anthrax disease in adults at high risk of exposure. FDA

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01237 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.855

could issue an Emergency Use Authorization to permit use of this vaccine for post-exposure prophylaxis if the criteria for issuance are met. HHS procured 28.75 million doses of anthrax vaccine in 2005 and 2007 for $691 million. In addition, HHS has funded studies to support longer expiration dating (3→4years) and to support the post-exposure prophylaxis indication. In 2008, CDC procured an additional 14.5 million doses of BioThrax at $404.7 million. There was a modification to the FY 2009 contract in April 2011 that added 3.42M doses at a cost of $101M, which brought the overall deliveries to that contract to nearly 18M doses. Most recently, CDC awarded a contract to Emergent for acquisition of this product over the next five years. In September 2011, CDC procured 44.75 million doses of its anthrax vaccine, worth up to $1.25 billion over five years.

Is there a commitment to moving forward with a second generation vaccine? If so, how much funding is necessary to get it done and what is your time frame for doing so?

Yes. In addition to supporting the existing BioThrax vaccine from Emergent, HHS supports the development of next generation anthrax vaccines. BARDA supports the advanced development of four (4) next generation anthrax vaccine candidates based on recombinant protective antigen (rPA). Three next generation vaccine candidates (Emergent, Pfenex, and PharmAthene) express the rPA protein in different bacterial expression systems and all are administered intramuscularly; a fourth candidate (Vaxin) is administered intranasally using an adenovirus-based vector system. Since 2007, BARDA has provided $168 million to support development of these next generation anthrax vaccine candidates. Furthermore, BARDA and NIAID are supporting studies using both the licensed AVA and rPA vaccine candidates using new adjuvants (e.g., CpG) that may provide greater immunity with fewer doses and less antigen per dose.

Currently vaccine development routinely takes 8-10 years at a cost of $0.8 – 1.2 billion. Based on the current stage of early development for the BARDA-supported next generation anthrax vaccine candidates, funding will be needed for another 6-8 years for further development of this early stage research. Provided that one or more next generation anthrax vaccine candidates proceed successfully to late stage development, vaccine procurement may be warranted.

4. **At a House Energy and Commerce Subcommittee hearing in July, you stated that this old vaccine was not ideal in the event of an emergency because it requires multiple doses over 18 months to confer immunity. My understanding is that there are additional drawbacks to this product including complaints from military recipients and a history of safety concerns. In fact, in June, your department classified one of the preservatives used in the vaccine as a known carcinogen, making it totally unsuitable for children, if not adults. Given that the product does not meet the needs of the existing requirement, why has HHS spent billions on this product since 2005?**

In the absence of a stable and immunogenic next generation anthrax vaccine in late stage development, the federal government has procured BioThrax, also known as anthrax vaccine adsorbed (AVA), which is licensed in the United States as a five-dose regimen to prevent anthrax disease. The vaccine has been demonstrated safe and effective for this indication. At a National Biodefense Science Board meeting in 2011, experts stated that the safety profile of BioThrax is comparable to other currently licensed vaccines. Previous adverse event

67123.856

complaints against BioThrax resulted from the subcutaneous route of administration of the vaccine. The change from subcutaneous to intramuscular route of administration has reduced significantly the local pain, redness, and induration experienced at the site of injection. Additionally, three (3) injections are recommended for post-event prophylaxis rather than the five (5) injections, with annual boosters, administered for military vaccinations for prevention of anthrax disease. Also HHS is supporting studies using anthrax vaccine candidates formulated with new adjuvants that may reduce the number of required doses even further. Lastly, HHS is supporting development of next generation injectable anthrax vaccines that may have fewer localized adverse reactions than BioThrax; another next generation anthrax vaccine under development may be administered intranasally rather than intramuscularly.

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Ten Years After 9/11: The Next Wave in Aviation Security
Chairman Joe Lieberman
November 2, 2011

Good morning and welcome to our hearing. Today we will take stock of our efforts over the past 10 years to secure aviation travel, and to discuss where we must go from here to make the system more secure, more efficient, and, if possible, more convenient for the majority of travelers, without diminishing security.

I want to thank TSA Administrator John Pistole, who has spent a lifetime in service to the security of our nation, and our other witnesses for being here today.

Today is the 11th and final hearing in our Committee's yearlong, "Ten Years After 9/11" series examining reforms made over the last decade to government operations that failed us in the years leading up to 9/11.

Most of the reforms we've examined – from intelligence coordination, to preventing terrorists from entering the country, to emergency communications – have improved significantly since 9/11. But the risks we face today have changed significantly since 9/11. So, the successes we have had in the war on terror - including the strikes against Osama bin Laden and Anwar al-Awlaki, and numerous plots against our homeland that have been thwarted – do not diminish the need to carry on our efforts to stay one step ahead of our enemies' changing plans for attacking us.

Aviation security was, of course, one of the greatest failures that enabled the Islamist terrorists to attack us on 9/11. And air travel remains on our terrorist enemies' top list of priorities for attack. Therefore aviation security is one of the first areas we set out to fix. Congress moved quickly in the fall of 2001 to close the most glaring security gaps. We immediately hardened cockpit doors to prevent hijackings. We created the Transportation Security Administration (TSA) to replace private sector airport screeners with federal employees who would be held to strict security standards.

TSA revamped the way passengers were screened, and adapted again and again as terrorists tried to defeat the latest security measure TSA put into place. When Richard Reid tried to ignite explosives in his sneakers aboard an airplane in 2002, TSA asked passengers to remove their shoes for screening. When a plot was uncovered in 2006 to blow up planes with liquid explosives, TSA restricted liquids brought on board planes. When the Christmas Day bomber tried to blow up a plane with well-concealed plastic explosives in 2009, TSA stepped up its physical pat downs of passengers and increased the use of whole body imaging machines. And when terrorists tried to pack a bomb in a toner cartridge to be placed onboard a cargo plane, TSA limited the amount of ink or toner that can be transported on cargo planes.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel: (202) 224-2627 Web: http://hsgac.senate.gov

67123.858

TSA screens 2 million air passengers and their luggage each day using technology that continues to improve– from metal detectors to backscatter x-rays to explosives trace detectors to whole-body imaging machines. Since 9/11, DHS has also improved its ability to prescreen passenger lists against government watchlists and use behavioral profiling to detect passengers with evil intentions before they board a plane. The Department has also increased the number of Federal Air Marshals on domestic and international flights, and continues to work closely with our foreign partners to raise screening standards for flights originating abroad.

Cargo security, too, has been improved greatly since 9/11. All cargo on domestic passenger flights is screened before loading. On international flights, cargo details were not required until after a plane had taken off, but before it arrived in the U.S. The printer and ink cartridge plot, however, rendered that timeline meaningless. Clearly, we need to obtain shipping data before the departure of any international flight heading to the U.S. if we are to stop cargo bombs.

For that reason, DHS has begun working with shippers and air carriers to obtain descriptions of cargo earlier in the process so the Department can determine the risk and therefore the type of screening needed. Senator Collins and I are working on legislation that would require data to be collected on all cargo shipments before they are loaded onto planes, so that we can be assured that all high risk cargo can be screened properly before it is airborne.

The past decade has seen dramatic improvement in our aviation security. We have spent billions of dollars building multi-layered defense systems to prevent terrorists and explosives from getting on airplanes. And though we have improved security significantly, we seem to be better at playing catch up, reacting to the most recent terrorist tactic, rather than anticipating what might come next, and putting appropriate safeguards in place.

In order to avoid another "failure of imagination", as the 9/11 Commission warned in its 2004 report, DHS and TSA need to think creatively about better uses of technology and information in the screening process.

So, the focus of my questions for our witnesses today is how can we better address the vulnerabilities that remain in our aviation security systems and how can we make the system more efficient and convenient without jeopardizing security?

67123.859

United States Senate
Committee on Homeland Security and Governmental Affairs
Senator Susan M. Collins

Contact: E.R. Anderson 202-224-4751

Opening Statement of Senator Susan M. Collins

Ten Years After 9/11: Next Wave in Aviation Security

Committee on Homeland Security and Governmental Affairs
November 2, 2011

By targeting our airplanes, al Qaeda succeeded in killing nearly 3,000 people. Aviation security is clearly critical to homeland security.

We Americans have demonstrated our willingness to endure enhanced security measures at our airports -- if those measures appear reasonable and related to the real risks. But travelers become frustrated when security measures inconvenience them without cause, or when they appear to be focused on those who pose no threat.

Next month, it will be 10 years since the shoe bomber failed to take down his flight from Paris bound for Miami. Yet, we still take off our shoes.

In 2006, British and American intelligence thwarted an attempt to conceal explosives in liquid bottles. We still can't carry a regular-size tube of toothpaste onto an airplane.

The Christmas Day bomber hid explosives in his underwear, and media reports indicate that terrorists have shown interest in having explosive devices surgically implanted in their bodies. These threats have led to more intrusive pat-down searches, and one wonders what more will be required of airline passengers in the future.

We see TSA putting the very young and the elderly through intrusive, and in most cases unnecessary, screenings.

At the same time, it troubles many Americans to learn that a young man was able to fly cross-country without a valid government ID and with an expired boarding pass that was not even in his name.

If we continue to give extra screening to individuals who pose no threat, yet others who should arouse suspicion can get past check points without being questioned, our systems are still not working as they should.

Since our June hearing, the Administration has implemented a risk analysis to improve the screening process, a welcome change. This effort should provide a more effective and efficient use of the government's limited screening resources.

I am encouraged, for example, that this new risk-based approach is designed to permit TSA to learn more about travelers through information they choose to provide.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01242 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.860

Some of the changes will also answer several of our common airport screening complaints. Secretary Napolitano said in September that frequent fliers who opt-in to a known-traveler program will often get to keep their shoes on and their lap tops in the bags. TSA has also changed the screening procedures for children under 12 -- a commonsense decision that was overdue.

Nevertheless, questions remain regarding how some security procedures affect Americans' privacy.

In August, TSA began installing new software in passenger screening machines designed to enhance traveler privacy. Using a generic outline of passengers, Automated Target Recognition detects items that could pose a potential threat.

I first saw this less invasive technology in Amsterdam in 2010 and repeatedly raised the issue with Administrator Pistole and Secretary Napolitano. I urged consideration of this software that better respects travelers' privacy and eliminates inconsistencies associated with human reviewers. I am pleased that this is finally the direction TSA is headed.

While ATR technology is currently being used with so-called "millimeter wave" machines, which use Radio Frequency energy to generate images, I would note that other Advanced Imaging Technology screening machines that use "backscatter" x-ray radiation have continued to raise health concerns. DHS should independently evaluate the health effects of that technology and establish a goal of using radiation-free screening technology.

Let me underscore my appreciation of the fact that no single screening technology can ensure our safety. A layered screening system is essential. We face a determined foe, and no machines can substitute for good intelligence, well-trained screeners, and an observant public.

The passenger screening process has received both attention and sometimes anger from the traveling public. It became clear last year, however, from the printer cartridge plot that cargo security is also a threat the terrorists are probing. This is why Senator Lieberman and I intend to introduce an Air Cargo Security bill later this year. Our successes in the risk-based screening of maritime cargo should provide a road map for risk-based screening of air cargo. And that is what our legislation is intended to do.

Our government's first priority is to protect against terrorism, and the public will accept a certain level of intrusion and inconvenience at our airports. But DHS should continue to expand the use of risk-based approaches to screening with technology and techniques that are safe and effective and that minimize privacy and health concerns.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01243 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.861

Prepared Statement of Senator Mary L. Landrieu
"Ten Years After 9/11: The Next Wave in Aviation Security"
Committee on Homeland Security and Governmental Affairs
November 2, 2011

In the aftermath of 9/11, Congress established a new federal agency to protect the flying public from future acts of terrorism. And while the Transportation Security Agency has succeeded in preventing another coordinated attack against the United States, its security achievements have taken a severe toll on efficiency and privacy - some might even say dignity.

Americans are accustomed to showing their boarding pass, ID, and walking through a metal detector at the airport, but in the course of the last few years, successive terrorist plots that we've uncovered have prompted additional requirements. Travelers must now remove their shoes, coats, laptops, liquids, and completely empty their pockets before undergoing explosive scans, hand swabs, secondary bag inspections, and the notorious pat-downs.

Balancing security with privacy is not a new challenge in the realm of homeland security, but the TSA is unique because the average American citizen interacts with Transportation Security Officers more than any other segment of the federal workforce, which means that TSA employees and procedures have a profound impact on people's impression of the federal government as a whole. So when infants and elderly women are patted down and wheelchairs are taken apart, people feel that their government is behaving in an intrusive and insensitive fashion, and what's more, they are not even realizing a security benefit for all that trouble given the low-level threat posed by these populations.

A 2010 survey by Consensus Research concluded that American travelers would take 2 to 3 additional flights each year if the hassles of security screening were eliminated. That would translate into an additional $85 billion in consumer spending and 900,000 jobs in the United States. The same study found that a majority of respondents consider the current system to be "inconsistent," "stressful," and "embarrassing."

Richard Reid, the Underwear Bomber, and the Heathrow and UPS cargo plots are all evidence that Al Qaeda and its affiliates still seek to blow up commercial and cargo jets, so we cannot afford to let our guard down. But that doesn't mean we can't develop a smarter system that provides both security *and* convenience. Technology and training are critical to achieving that dual objective. New equipment will protect privacy, expedite screening, and reduce manpower requirements. Better training will identify threats more effectively and improve the public's perception and trust in the agency overall.

The challenge inherited by TSA Administrator Pistole is immense. I met with him privately on March 11th and questioned him in front of this committee at a hearing on June 22nd about the agency's plans to bridge the huge divide between the current, one-size-fits-all system that treats each passenger as an equal threat, and a risk-based system for the future that is more cost-effective, user-friendly, and focused on credible threats. Mr. Pistole has demonstrated his willingness to simplify procedures and advance reforms by launching 6 important new initiatives that I would like to outline very briefly:

1) Deploying new ***Advanced Imaging Technology*** machines to more accurately detect explosives or anomalies without displaying revealing body images;
2) Using ***Automatic Target Recognition*** software to automate detection instead of requiring TSA personnel to view images on a screen;

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01244 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.862

3) A program called ***SPOT*** that uses Behavior Detection Officers instead of random selections to determine whether passengers must undergo secondary screening;
4) A pilot called ***Pre-Check*** that allows frequent flyers to keep their shoes and jackets on and their laptops and liquids in their bag if they complete a background check and register biometric data;
5) A pilot called ***Known Crewmember*** that allows airline pilots to forego screening if they're in the FAA database and show 2 forms of ID; and
6) A pilot called ***Credential Authentication Technology/Boarding Pass Screening Systems*** that will use electronic scanners to check IDs and boarding passes instead of requiring TSA officers to carry out this task.

So the TSA is making important strides, but it still has a long way to go, and the American people, the domestic travel and tourism industry, and I expect them to get it done. The 3 pilot programs that I just mentioned will only operate for a few months in a handful of airports, so the agency must review, tweak, and expand them as quickly as possible once their trial periods conclude.

This hearing is about finding ways to improve the experience of the flying public without unreasonable sacrifices in security. Financing these improvements is not the domain of the federal government alone; airport authorities, individuals, and airlines also play a role.

- ***Airports*** may need to re-design their facilities to accommodate the "Checkpoint of the Future."
- ***Passengers*** may be required to pay an increased security fee to offset the additional costs to acquire new technologies.
- ***Airlines***, whose security fees have not increased since 2001, may also be asked to help finance these improvements.

Airlines have suffered decreased passenger volume since 9/11 as a result of heightened security concerns, fuel prices, and the recession. But airlines have also contributed to the public's general frustration with the entire flying experience by charging a widening array of fees for very basic amenities. So now, in addition to undressing and being groped at security checkpoints, passengers are being forced to pay for checked baggage, carry-on baggage, and sufficient legroom.

Streamlining aviation screening will ultimately make us safer, save taxpayers money, uphold passengers' dignity, restore public confidence, increase throughput, and benefit the economy. As we move forward with TSA reforms, we must carefully consider how to allocate the costs of those improvements and evaluate security screening within the larger context of the public's overall experience. I look forward to working with Administrator Pistole, the industry organizations represented here today, and the members of this committee to accomplish these goals.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01245 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.863

Statement of

John Pistole

Administrator

Transportation Security Administration

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Governmental Affairs

November 2, 2011

Good morning Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. Thank you for the opportunity to testify today about the Transportation Security Administration's (TSA) on-going efforts to develop and implement a more risk-based approach to secure our nation's transportation systems. When I last appeared before this Committee this past June, our plans to implement additional risk-based security (RBS) measures were still in their formative stages. I am pleased to report that we have now begun operational testing of several key aspects of risk-based security that I will describe.

TSA employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. Our goal at all times is to maximize transportation security to stay ahead of evolving terrorist threats while protecting privacy and facilitating the flow of legitimate commerce. TSA's security measures create a multi-layered system of transportation security that mitigates risk. We continue to evolve our security approach by examining the procedures and technologies we use, how specific security procedures are carried out, and how screening is conducted.

Since I became TSA Administrator, I have listened to ideas from people all over this country, including our key stakeholders and security professionals, and I have heard from our dedicated workforce and our counterparts abroad about how TSA can work better and smarter.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01246 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.864

Based on this feedback, last fall, I directed the agency to begin developing a strategy for enhanced risk-based security (RBS), which is based on the simple premise of focusing our limited resources on the passengers we know least about. I am pleased to report to the Committee today that in the past few months we have taken concrete steps to implement key components of the agency's intelligence-driven, risk-based approach to security, advancing the agency toward the ultimate goal of providing the most effective security in the most efficient way possible.

TSA Pre✓™

This past October, TSA began testing a limited and voluntary passenger pre-screening initiative with a small known traveler population at four U.S. airports (Miami, Dallas-Ft. Worth, Detroit, and Atlanta). This pilot program will help assess measures designed to enhance security, by placing more focus on pre-screening individuals who volunteer information about themselves prior to flying in order to potentially expedite the travel experience. By learning more about travelers through information they voluntarily provide, and combining that information with our multi-layered system of aviation security, we can better focus our limited resources on higher-risk and unknown passengers. This new screening system holds great potential to strengthen security while significantly enhancing the travel experience, whenever possible, for passengers.

During this pilot, TSA is using pre-screening capabilities to make intelligence-based risk assessments for passengers who voluntarily participate in the TSA Pre✓™ program and are flying domestically from one of the four airport pilot sites. Eligible participants include certain frequent flyers from American Airlines and Delta Air Lines as well as existing members of U.S. Customs and Border Protection's (CBP) Trusted Traveler programs including Global Entry, SENTRI, and NEXUS who are U.S. citizens and are flying on participating airlines. The data collected from these pilot sites will inform our plans to expand the program to include additional airlines as well as other airports that participate in CBP's Global Entry program, once they are operationally ready.

TSA pre-screens TSA Pre✓™ passengers each time they fly through participating

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01247 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.865

airports. If the indicator embedded in their boarding pass reflects eligibility for expedited screening, the passenger is able to use TSA's Pre✓™ lane. Because we know more about these passengers, TSA Pre✓™ travelers are able to divest fewer items, which may include leaving on their shoes, jacket, and light outerwear, as well as other modifications to the standard screening process. As always, TSA will continue to incorporate random and unpredictable security measures throughout the security process. At no point are TSA Pre✓™ travelers guaranteed expedited screening.

Transportation Security Officers (TSOs) in the four pilot airports are receiving very positive feedback from TSA Pre✓™ travelers while the two partner airlines have successfully demonstrated the technical capabilities required to participate in the program, thus paving the way for other airlines to follow. As we learn from these pilots, we are working closely with other airlines and airports to determine when they may be operationally ready to join. We are also working with CBP to ensure that individuals who want to apply for Trusted Traveler Programs are able to do so in an efficient manner.

Known Crewmember

We hold airline pilots responsible for the safety of the traveling public every time they fly a plane. It makes sense to treat them as our trusted partners. To build on our risk-based approach to security, we are currently supporting efforts to test another identity-based system to enable TSA security officers to positively verify the identity and employment status of airplane pilots. The Known Crewmember program is the result of a joint test between the airline industry (Air Transport Association) and pilots (International Airline Pilots Association), which allows uniformed pilots from 22 airlines to show two forms of identification that are checked against a database called the "Cockpit Access Security System," which confirms identity. After more than two months into the pilot program, and with deployments nearly complete at the seven participating airports, over 59,000 uniformed pilots have been cleared through the process with an average of nearly 1,900 approvals per day. Both Known Crewmember and TSA Pre✓™ are clear examples of TSA's commitment to focusing its attention and resources on those who present the greatest risk, thereby improving security and the travel experience for passengers

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01248 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.866

across the country.

Expanded Behavior Detection

Beginning this fall, TSA took steps to expand its behavior detection program that builds on existing Screening of Passengers by Observation Techniques (SPOT), which has grown since 2003 to include over 160 airports. Under the pilot program, TSOs employ specialized behavioral analysis techniques to determine if a traveler should be referred for additional screening at the checkpoint. The vast majority of passengers at the pilot airport checkpoints experience a "casual greeting" conversation with a Behavior Detection Officer (BDO) as they pass through travel document verification. This additional interaction, used by security agencies worldwide, enables officers to better verify or dispel suspicious behavior and anomalies.

Preliminary analysis from Boston shows an increase in the rate of detection of high-risk passengers. However, additional data is required to understand if the trend seen in the Boston data is statistically significant and replicable at other airports. TSA is currently conducting analyses with the DHS Science and Technology Directorate to estimate the number of cases required for validation. In the meantime, we are expanding this pilot to Detroit in order to collect additional data on incorporating enhanced real-time risk assessments into our other layers of security.

Screening of Children 12 And Under

This past August, TSA modified its screening procedures to provide more options to resolve alarms that may occur during the screening process of passengers 12 and under. With nationwide rollout complete as of late September, the data has demonstrated a reduction – though not elimination – of the need for a physical pat-down for children that would otherwise have been conducted to resolve alarms. We maintain our standard procedure that when a pat-down is required of any minor, a parent or guardian must be present and the screening may occur in private. TSA has also implemented additional measures to expedite the screening process where possible including allowing passengers 12 and under to leave their shoes on.

By streamlining procedures for these lower risk passengers through programs like these,

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01249 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.867

TSA is better able to focus its finite resources on those who pose higher risks to transportation. We are continuously evaluating lessons learned from these modified procedures to determine our next steps as we consider future procedures to strengthen and streamline the security screening process for other low-risk populations.

New Document Assessment Technology

In addition to testing new procedures for low-risk populations, TSA is also employing technology to automatically verify passenger identification documents and boarding passes, providing TSA with a greater ability to identify altered or fraudulent documents. This technology, known as Credential Authentication Technology – Boarding Pass Scanning Systems (CAT-BPSS), will eventually replace the current procedure used by security officers to detect fraudulent or altered documents. CAT-BPSS enhances security and increases efficiency by automatically and concurrently comparing a passenger's ID and boarding pass to a set of security features to verify their authentication and ensure that the information on both match. The system also verifies the IDs of airline personnel and can screen a wide range of travel documents. TSA began testing the technology in July 2011 and will deploy and evaluate the technology at TSA Pre✓™ airports in the near future.

Conclusion

TSA will continue to enhance its layered security approach through state-of-the-art technologies, expanded use of existing and proven technology, better passenger identification techniques and other developments that will continue to strengthen aviation security. I thank you for the opportunity to appear before you today, and I look forward to answering your questions about the evolution of TSA's risk-based, intelligence-driven approach to security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01250 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.868

U.S. TRAVEL
ASSOCIATION

TESTIMONY FOR THE RECORD

OF

ROGER DOW, PRESIDENT AND CEO OF THE U.S. TRAVEL ASSOCIATION

ON

"TEN YEARS AFTER 9/11: THE NEXT WAVE IN AVIATION SECURITY"

BEFORE THE

SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

NOVEMBER 2, 2011

U.S. TRAVEL ASSOCIATION
1100 NEW YORK AVENUE, NW, SUITE 450
WASHINGTON, DC 20005-3934
202.408.8422
FAX 202.408.1255

67123.869

Chairman Lieberman, Ranking Member Collins and Members of the Senate Committee on Homeland Security and Governmental Affairs: I am pleased to offer testimony on behalf of the U.S. Travel Association (U.S. Travel).

I also want to thank you for your leadership of this Committee and for the dedication you have demonstrated over the years working in a bipartisan fashion to ensure the nation remains safe from future terrorist attacks while also understanding the need for effective travel facilitation. Chairman Lieberman, we will miss you in retirement, and thank you for your service in the Senate for so many years.

The U.S. Travel Association is the national, non-profit organization representing all sectors of America's $1.8 trillion dollar travel industry. U.S. Travel's mission is to increase travel to and within the United States.

As you all know, travel is a powerful engine of growth and economic development. For example, travel directly employs more than 62,000 people in Connecticut, contributes $8.8 billion dollars annually to the Connecticut economy and generates more than $1.4 billion dollars in state and local tax revenues. Similarly, travel directly employs more than 30,000 people in Maine, contributes more than $2.7 billion dollars to the state's economy and generates nearly $334 million dollars in state and local tax receipts. In every state and county across America, travel helps pay the salaries of police, firefighters and teachers without creating new demand for those public services. Travel industry investments, such as airports, hotels and convention centers, attract additional private-sector investments that, together, sustain communities and help them grow.

While the topic of aviation security is often discussed in the context of terrorism, personal privacy or technology – less attention is paid to the economic damage inflicted by the current inefficiencies in the passenger screening process. For the travel community – which supports rural and urban communities alike – inefficiencies in the aviation security screening process impose a staggering cost on the economy, hampering job creation and economic growth. And the data suggests that the problem is getting worse.

A 2008 survey of air travelers who took one or more flights in the previous year found that one in four respondents (28 percent) avoided at least one trip because of the hassles of air travel, which include aviation congestion and passenger screening. That loss of travel translates into a $26.5 billion dollar loss to the U.S. economy, including $9.4 billion to airlines, $5.6 billion to hotels, $3.1 billion to restaurants and $4.2 billion in federal, state and local tax revenue.

Compare that $26 billion dollar loss to a 2010 survey conducted by Consensus Research, which found that American travelers would take an additional two to three flights per year if the hassles in security screening were eliminated. These additional flights would add nearly $85 billion in consumer spending and support 900,000 American jobs.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01252 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.870

The budgetary costs of TSA are also ballooning at a time when we are looking for ways to be more fiscally responsible and air travel is expanding. Since 2004, TSA's overall budget has increased by 68 percent. During the same time period, passenger levels have remained almost the same – with 618 million air passengers in 2004 and 623 million air passengers in 2010. This current trend cannot be maintained as TSA is spending more money each year to screen the same amount of passengers. And the problem will only get worse. The FAA now predicts that in 10 years (by the year 2021) there will be 1 billion U.S. air travelers per year.

Beyond the numbers is the empirical evidence. Most of you fly every week. You can see for yourselves the friction and inefficiencies in the system.

I want to talk to you today about what reforms can be made to the aviation security system to help stimulate the economy. The current system has reduced threats and helped to ensure passenger safety; but it is inefficient, and "the hassle factor" for travelers is at an all-time high.

We know there is a better way. And to start – we must rid ourselves of the Hobson's choice that we cannot have security and traveler facilitation simultaneously.

That is why in 2009 U.S. Travel convened a blue ribbon panel of bipartisan, aviation security and industry experts – including former Secretary of Homeland Security Tom Ridge, former Congressman Jim Turner, and Sam Gilliland, CEO of Sabre Holdings – to review the U.S. air travel security system and recommend reforms for creating a more efficient, secure and traveler-focused system. After a year of discussions and over 20 meetings, U.S. Travel issued a report, "A Better Way: Building a World Class System for Aviation Security," which presents a comprehensive review of aviation security and takes account of the traveler's point of view.

The report lays out a comprehensive checklist of 14 recommendations that give Congress and TSA a roadmap for aviation security reform that will maintain security while improving passenger facilitation.

While each of the blue ribbon panel's recommendations is important, I would like to focus today on three of the panel's key recommendations: 1) creating a risk-based trusted traveler program; 2) steps to decrease the number of carry-on bags; and 3) reconstitution of the Aviation Security Advisory Committee.

First, the top recommendation of the blue ribbon panel was that Congress and TSA must work together to create a broad, risk-based trusted traveler program.

The need for this program is clear. The current "one-size-fits-all" screening process at America's airports does not meet the needs of the traveling public. Travelers have no input or choices. In our view, a trusted traveler program would allow travelers to opt-in and voluntarily provide background information, and qualify for predictable, expedited screening as long as they meet certain criteria to establish their low-risk nature.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01253 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.871

The blue ribbon panel recommended three elements of a trusted traveler program that utilize a risk-management approach. These elements are: 1) a secure and accessible enrollment and re-verification process that encourages a large number of enrollees; 2) dedicated screening lanes for trusted travelers and a confirmation process at the airport that ensures only enrollees are utilizing these lanes; and 3) a screening process that provides efficiency, security benefits, and an acceptable level of predictably. We strongly believe all three elements are achievable.

Not long after the release of our report, our team met with Administrator Pistole's team at TSA to discuss this proposal and get their feedback. During that meeting, we learned of several initiatives that were underway to reform TSA into a more risk-based and intelligence driven organization. To the credit of Administrator Pistole and the leadership team at TSA, one of the central reforms was to create a risk-based screening program. I applaud him for his leadership and vision in undertaking this effort and for launching the PreCheck pilot program. I also applaud you and others in Congress for also taking an interest in this critical issue and hope to work with you as you begin to oversee the implementation of TSA's efforts.

As Administrator Pistole mentioned, TSA recently began a pilot program called PreCheck with the goal of providing expedited screening for passengers willing to volunteer more personal information. PreCheck is currently being run at four airports and passengers can enroll in the program by being a member of a Customs and Border Protection's (CBP) trusted traveler program or by sharing personal information contained in Delta or American frequent flyer accounts.

As TSA examines how to expand the program, we believe the agency and Congress should take into account several key issues:

- Allow for broad enrollment into the program;
- Provide dedicated PreCheck screening lanes at major U.S. airports; and
- Develop a screening process that creates efficiencies, improves security, and provides a predictable time for enrollees to move thru screening, even if the actual screening procedures vary to provide a needed degree of randomness.

First, in order for PreCheck to succeed, it must maintain security while allowing enough travelers to enroll to make the standard security screening line shorter and more efficient for travelers not participating in the program. We believe this will require TSA to allow travelers to aggregate their frequent flyer miles across multiple airlines, so that more travelers can meet the minimum threshold of miles to join PreCheck. We believe this will also require TSA to expand enrollment opportunities beyond frequent flyer programs and CBP trusted travelers. TSA should examine using commercial data, criminal history, or Registered Traveler providers as other means of enrolling passengers in PreCheck. In addition, TSA should seek to enroll existing populations of low-risk travelers into PreCheck, including persons with Top Secret clearances, Security Identification Display Area (SIDA) badges or Transportation Worker Identification Credential (TWIC) cards.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01254 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.872

Second, as the PreCheck program grows, TSA should provide dedicated screening lanes for all PreCheck enrollees. TSA – in consultation with airports and airlines – should determine where PreCheck screening lanes will be available and base these decisions on efficiency and security.

Third, Administrator Pistole has stated on a number of occasions that PreCheck enrollees will be randomly selected for additional screening, instead of the expedited screening. This is a sensible and prudent security measure. However, if PreCheck enrollees are selected for additional screening during a high percentage of their trips, they will still be forced to arrive at the airport well in advance of their flight in order to plan for the likelihood of increased wait times. In that scenario, PreCheck passengers would likely see the program as providing little efficiency benefit. Therefore, TSA should seek to use enrollment criteria that provides the best indication of risk and allows PreCheck enrollees with predictable wait times in the screening process - even if the actual screening procedures vary to provide a needed degree of randomness.

The U.S. Travel Association looks forward to working with TSA and Congress to ensure the growth and success of the PreCheck program.

I would now like to turn to the second key recommendation of the blue ribbon panel – Congress and TSA must find ways to encourage fewer carry-on bags. The recent trend of most airlines charging separate fees for every checked bag has resulted in airline passengers "carrying on" substantially more baggage per person. The increase volume of carryon baggage is causing significant checkpoint congestion, negatively impacting security, and causing significant strains on TSA personnel and resources.

The numbers speak for themselves. The New York Times recently reported that TSA screened an estimated 59 million more carryon bags in 2010 than in 2009.[1] TSA also estimates that carry-on bags processed at the checkpoints will have increased by about 87 million from FY 2010 through FY 2011 and continue to increase by about 29 million more in FY 2012.

The blue ribbon panel proposed to deal with this problem by requiring that airlines include one checked bag as part of the base fare of an airline ticket. This would give passengers the option to check a bag that the security checkpoints are not overwhelmed by continued increases in carryon luggage. It is important to note that under the panel's recommendation, passengers would not be entitled to a free checked bag. Airlines would be able to cover the costs of checking one bag in the base fare of the ticket and set that price to whatever level they desire.

A 2011 survey conducted Equation Research found that travelers would likely change their behavior if such a proposal was enacted. The survey showed that two-thirds of travelers would be willing to carry on one less item if it meant being able to check one item at no extra fee.

[1] http://www.nytimes.com/2011/03/29/business/29bags.html

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01255 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.873

The last recommendation of the blue ribbon panel that I will highlight today is the need for TSA to reinstate the Aviation Security Advisory Committee (ASAC) to consistently engage a broad group of stakeholders when crafting aviation security policy. For almost two decades, the Federal Aviation Administration (FAA) and then TSA operated the ASAC, which engaged a wide array of interested stakeholders in a dialogue on aviation security issues and policies. The ASAC members took the time to consider and learn difficult and technological issues, and made meaningful recommendations to the federal government. Unfortunately, since 2006, TSA has not convened a meeting of the ASAC, thereby cutting off a valuable tool for TSA to engage the travel industry and a broad range of stakeholders.

In July 2011, TSA announced that it would reconstitute the ASAC and the travel industry is anxiously waiting to hear if a representative from the industry will be appointed to that committee. Congress can also play an important role in this process by codifying the ASAC's structure and mandate. By requiring that a broad group of stakeholders – including the travel industry – be represented on the ASAC, Congress can help ensure that TSA is making informed policy decisions that maintain security while better facilitating passengers and commerce. For far too long the voice of the travel industry and the traveler have not been "at the table" in the construction of aviation security policy. That is why the reconstitution of the ASAC is so important and why it is equally important that you have invited the travel industry to participate in this hearing today.

It is my hope that Congress and TSA will consider these and other recommendations provided by the blue ribbon panel. The ideas contained in the report do not constitute the last word in aviation security policy, but they are intended to spark the conversation for reform. I am pleased to be provided the opportunity to share them with you today and appreciate hearing your feedback.

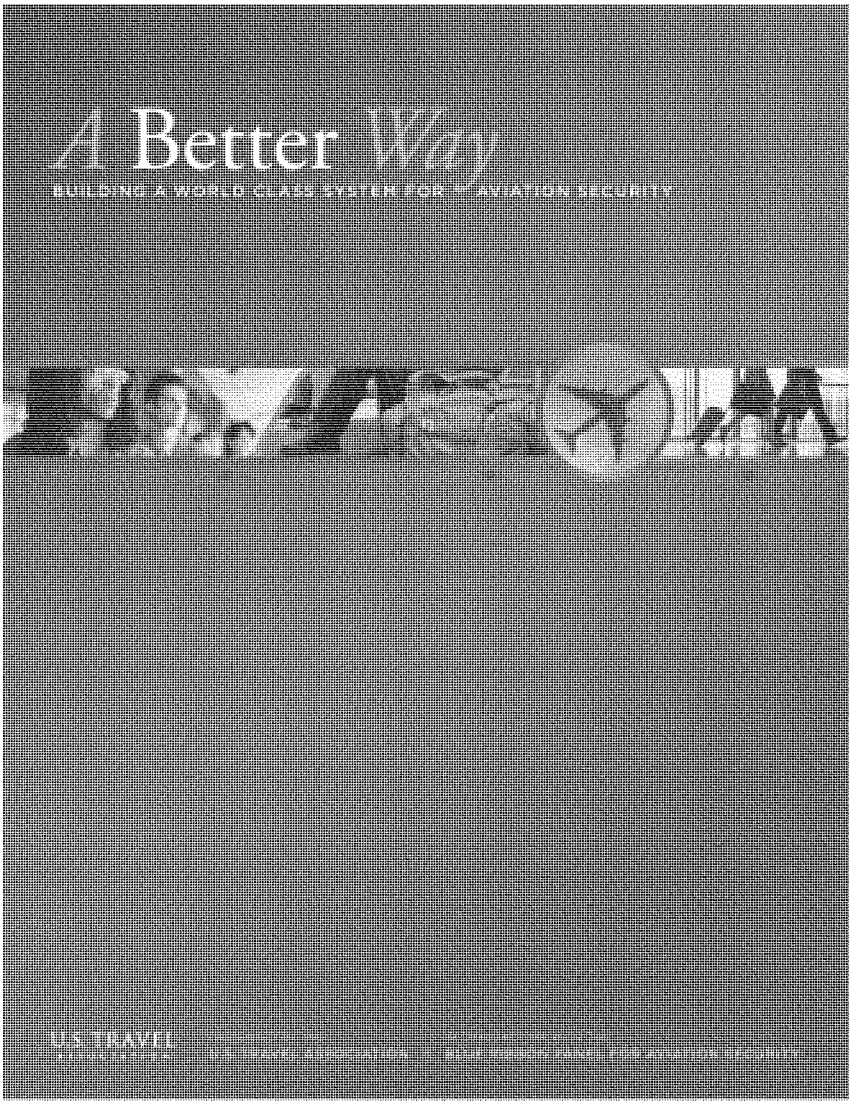
I believe that as we continue identify ways to keep our nation safe from those intent on doing our country harm, we must define success not only by measurements of security, but also by measurements of efficiency and customer satisfaction. From PreCheck, to standard screening procedures, to employee training, TSA must measure and seek to improve customer satisfaction levels across all of its programs. Only then can TSA fulfill its dual mandate to protect our transportation systems <u>and</u> facilitate the movement of people and commerce.

In sum, while the security of America's air travel system and the safety of the passengers who use that system must remain everyone's overriding concern, it is possible to make the system more efficient and more convenient for travelers. This will be a win-win for American economy and the traveling public.

I thank Chairman Lieberman, Ranking Member Collins, and all Members of the Committee on Homeland Security and Governmental Affairs for holding this important hearing. And I thank you for the opportunity to testify before you today. I would be happy to answer any questions you might have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01256 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.874


A Better Way
BUILDING A WORLD CLASS SYSTEM FOR AVIATION SECURITY
U.S. TRAVEL

Executive Summary

Each day in the United States, roughly two million air travelers are advised to arrive upwards of two hours before a flight in order to be processed through a one-size-fits-all security screening system. Each traveler must present their identification for verification, take off any coats, remove their shoes, pull out their cell phone, unpack their laptop, unhook their belt, unsnap their watch, place their liquids in a clear plastic bag, and place all of their personal effects on a conveyer belt. Then, every man, woman and child goes barefoot through a screening device and then tries to reassemble their belongings before the crush of passengers further backs up the screening line.

Has the system worked? By one measure—yes. There have been no successful terrorist attacks against an American aircraft since the horrible events of September 11, 2001. If terrorist attacks are the only form of judgment, the post-9/11 security screening system has succeeded to date. The Department of Homeland Security (DHS), its Transportation Security Administration (TSA), and the American public with its new "take charge" attitude all deserve credit and our appreciation.

Is today's security screening system the most cost effective and efficient that the United States can possibly produce? No. The country that put a man on the moon, invented the Internet and creates daily innovations in manufacturing can and must do better.

Staggering Economic Consequences of the Current Security System

The current aviation security system is discouraging Americans from flying and contributing to a decline in productivity among those who choose to fly. According to a 2010 survey conducted by Consensus Research, American travelers would take an additional two to three flights per year if the hassles in security screening system were eliminated. These additional flights would add nearly $85 billion in consumer spending and 900,000 jobs to the American economy.[1]

According to the same research, a large majority of Americans consider today's security screening system to be "inconsistent," "stressful" and "embarrassing." The President of the United States acknowledged the challenges with today's system when he joked in the 2011 State of the Union address that we should support high-speed rail as an alternative to flying because, "it will be faster than flying—without the pat-down."[2]

In 1999, Supreme Court Justice John Paul Stevens wrote in the landmark case Saenz vs. Roe that the Constitution protects the right to travel freely within the United States and to be treated as a welcome visitor rather than a hostile stranger.[3] In 1958, Supreme Court Justice William O. Douglas, in holding that the federal government could not restrict the right to travel without due process, wrote:

"Freedom of movement across frontiers in either direction, and inside frontiers as well, was a part of our heritage. Travel abroad, like travel within the country…may be as close to the heart of the individual as the choice of what he eats, or wears, or reads. Freedom of movement is basic in our scheme of values."[4]

These powerful words, combined with the clear consequences of today's security screening system, highlight the need for more efficiency and cost effectiveness. Aviation security is about much more than providing for the safety of the traveling public—it is about protecting the American way of life.

When combining the staggering economic consequences of the current system with the widely held views of the traveling public—and with the American way of life hanging in the balance—the picture becomes clear: we can, and must, build a new traveler-focused system for aviation security.

A Better System Eliminates One-Size-Fits-All Approach

A better aviation security screening system must feature several characteristics, including:

- Effective methods of deterring and interdicting terrorist and criminal actors;
- Tailored security based upon risk assessment;
- Predictability for the traveling public; and
- Reasonable efficiency and cost-effective use of resources.

Building such a system will require the active participation of, and possible sacrifices by:

- Airlines;
- Airports;
- The broader travel industry;
- The traveling public;
- Federal agencies; and
- Congress.

Congress Must Lead the Way to Better Aviation Security

In November 2010, new enhanced "pat down" techniques and advanced "full-body scanning" equipment sparked a media

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01258 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.890

Executive Summary

frenzy over aviation security. A renewed public debate took place over the role of privacy in aviation security, and many in Congress and the media openly questioned if TSA had gone too far.

This outcry was an example of the wild swings in media coverage and public policy that, over the past 10 years, have characterized the debate over aviation security.

The "whipsaw" nature of security policy is best demonstrated by two recent Congressional actions. In June 2009, the House of Representatives rejected whole-body imaging machines as a primary means of screening travelers by a vote of 310-118. Just six months later, Congress abruptly accelerated and expanded the deployment of whole-body imaging machines for primary screening.[5] What changed? The unsuccessful attempt to destroy a Northwest Airlines plane on Christmas Day.

Dramatic policy shifts undermine the ability of our nation to create a secure and efficient aviation system, and demonstrate a lack of a long-term vision for aviation security. Furthermore, TSA and its Transportation Security Officers (TSOs) often bear unjustified public criticism for simply carrying out the ever-changing policies set by Congress and the Administration.

If this pattern is to change, Congress must set the tone and take on the responsibility of improving the current system. As the elected representatives of the American people charged with providing a check and a balance on the Executive Branch, Congress that must take the lead in coalescing all stakeholders in aviation security to enact meaningful reforms.

Some in Congress appear to have calculated that there are no political consequences to an inefficient and costly system, but great political consequences to a successful terrorist attack. This is a classic Hobson's Choice that the American traveling public repudiates. The debate Congress must engage in is not strong security versus weak security, but rather how to create a world class aviation security system that effectively manages risk, increases efficiency and embraces the freedom to travel.

The Blue Ribbon Panel: Expertise and the First Step toward Reform

In an effort to spark a productive dialogue and begin the process of reform, the U.S. Travel Association brought together a Blue Ribbon Panel for Aviation Security. The panel consisted of former top officials from DHS and TSA; representatives from the airline, airport, logistics and security technology sectors; and leaders who represent the destinations and other businesses reliant on a functional air travel system.

The Panel was asked to: 1) think beyond today's security process; 2) understand the dual need for security and efficiency; and 3) keep the interests of travelers in mind, including reasonable privacy and efficiency concerns.

The Panel was led by three co-chairs:

- The Honorable Tom Ridge, former Secretary of the Department of Homeland Security, currently CEO of Ridge Global;
- The Honorable Jim Turner, former Ranking Democratic Member of the House Homeland Security Committee, currently Partner at Arnold & Porter; and
- Mr. Sam Gilliland, Chairman and CEO of Sabre Holdings

The strength of the Blue Ribbon Panel was rooted in the diverse professional and political viewpoints of the panelists. And, as with any difficult issue, this diversity did not always lead to consensus. Throughout the report, panel member support for specific recommendations is noted by the blue dialogue boxes. The panel co-chairs, in particular, provided numerous hours of their time to discuss, deliberate and develop many of the recommendations below.

Garnering the Voice of the Traveler

An important but often overlooked voice in the security process is that of the traveler. To remedy this omission, the U.S. Travel Association canvassed travelers for insights on how to improve the system through opinion surveys and a new website, YourTravelVoice.org, which gathered approximately 3,000 recommendations, some of which are reflected in this report.

Recommendations

Unlike other reports on this topic that examine the issue from a single vantage point (such as privacy, airline profitability, or government spending), the recommendations below represent a unique merger of non-partisan views of all essential stakeholders in aviation security. Based on the advice of the panel experts and the views of thousands of travelers, the U.S. Travel Association makes the following recommendations:

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01259 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.891

GOAL NUMBER ONE — Improve the TSA checkpoint by increasing efficiency, decreasing passenger wait times and screening passengers based on risk

- **Implement a risk-based Trusted Traveler program.** Congress should authorize TSA to implement a new, voluntary, government-run Trusted Traveler program that utilizes a risk-based approach to checkpoint screening, with the goal of refocusing resources on the highest risk passengers;
- **Give TSA authority over entire checkpoint area.** Congress should immediately act to clear up confusion over "ownership" of commercial aviation security and authorize TSA to control the entire security checkpoint starting at the beginning of the security lines and ending after a traveler exits the screening area;
- **Improve preparation of travelers.** Industry stakeholders should work with TSA to improve their education and communication on security rules and regulations, targeting locations and sources that travelers are likely to review as they book or prepare for a trip;
- **Encourage fewer carry-on bags.** The Department of Transportation (DOT) should issue regulations requiring airlines to allow passengers one checked bag as part of their base airfare and standardize existing rules covering the quantity and size of items that can be carried onto an airplane.

GOAL NUMBER TWO — Improve governmental efficiency and cooperation in the execution of its security responsibilities

- **Reinstitute the Aviation Security Advisory Committee.** DHS should immediately reinstate and appoint the Aviation Security Advisory Committee to provide effective private sector input to DHS on aviation security within 180 days. DHS should also convene airport-specific working groups to identify and resolve problems affecting travelers at particular locations;
- **Facilitate non-partisan leadership of TSA.** The TSA Administrator should be converted to a five-year position extending across presidential administrations to be filled by a non-partisan official with expertise in both security and facilitation;
- **Develop a comprehensive technology procurement strategy.** TSA, in collaboration with technology vendors and the travel community, should develop a comprehensive strategy for implementing necessary checkpoint technology capabilities. Congress should provide multi-year funding plans for TSA to execute this strategy;
- **Encourage wider use of secure identification documents.** Federal and state governments should embrace programs that build and deploy secure identification documents in order to provide higher-quality identity documents to the traveling public that meet government security requirements;
- **Reduce duplicative TSA screening for international arrivals.** DHS should enable certain low-risk passengers who are traveling to another domestic airport to forego checked baggage and passenger screening upon landing in the U.S.;
- **Expand trusted traveler programs to qualified international passengers.** DHS should expand access to international trusted traveler programs for international passengers entering the U.S., as well as lead efforts to establish a multinational network of streamlined entry procedures for low-risk travelers;
- **Eliminate duplication between TSA and Customs and Border Protection (CBP).** DHS should streamline its operations at U.S. international airports to reduce unnecessary duplication and leverages CBP and TSA resources, authorities, and capabilities;
- **Push for international cooperation with U.S. security standards.** The federal government must continue to push for international cooperation in the development of international aviation security, including both bilateral and multilateral approaches, as well as with organizations such as the International Civil Aviation Organization (ICAO), to strengthen aviation security efforts while promoting travel and protecting travelers' rights;

GOAL NUMBER THREE — Restructure our national approach to aviation security by developing and utilizing real risk management methods and tools

- **Implement well-defined risk management processes.** The Administration should convene an external panel of experts with appropriate security clearances to review TSA aviation security programs, assess the risk each is designed to mitigate and develop metrics for measuring progress to lessen that risk.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01260 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.892

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01261 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.893

Impacts of the Current Aviation Security System

"I truly don't want to fly anymore. It used to be fun! I even got into the travel industry so I could help others do it for less, and they could feel the rush and exhilaration of a last-minute trip to anywhere. I'm all for security measures but I'm highly suspicious that this actually catches the people we're supposedly looking for. Now, we're spending money on things that make me hate what I used to love."

– A.K., *YourTravelVoice.org, 11/18/2010*

The United States air transportation system is a critical component of our country's transportation infrastructure and essential to U.S. economic vitality. A widely accessible air transportation system allows business and leisure travelers to access markets and destinations that are troublesome or impractical to reach by other modes of transportation, while providing quicker access to destinations in close proximity to a traveler's point of origin. By facilitating the movement of goods and people, air transportation enhances commerce, connects people and communities, and provides Americans with a better quality of life.

Civil aviation is vital to the travel and tourism industry. In 2007, civil aviation accounted for over $1.3 trillion in economic activity, or 5.6 percent of the total U.S. economy, and employed 11 million Americans in aviation-related fields.[6] In 2009, an estimated 701 million—or two million per day—domestic and international passenger trips were taken on commercial air carriers. The U.S. Department of Transportation (DOT) estimates that 12 percent of all leisure travel and 18 percent of all business travel is conducted using air transportation.[7]

Unfortunately, the same attributes that make civil aviation an essential part of our everyday lives also make it an attractive target for acts of terrorism. The events of September 11, 2001, demonstrated the devastating loss of life and the severe economic consequences that can be inflicted by a successful attack utilizing passenger aircraft.

After the attacks of 9/11, Congress and the federal government focused more resources and efforts on combating terrorism and protecting the homeland. The creation of DHS and TSA brought vast improvements to border and transportation security. Their efforts, in coordination with multiple federal, state and local agencies, have proved pivotal in deterring and preventing another large-scale terrorist attack on U.S. soil. As a result, there is little question that the U.S. is safer today than it was before 9/11.

However, as aviation security continues to evolve, the combination of new screening procedures, technologies, regulatory requirements, and evolving threats are putting increased strain on aviation stakeholders and the traveling public. Many are starting to question whether the current system strikes the proper balance between facilitating the movement of goods and people, and providing protection from the continued threat of terrorist attack.

The Economic Impact of Our Current Aviation Security System

According to a number of economic impact studies and consumer surveys, American business and leisure travelers face greater hassles, endure longer travel times, and lose economic opportunities as the result of the current airport security system. In fact, air traveler surveys conducted in 2008 and 2010 show that traveler frustration and the economic consequences of the current system are getting progressively worse.

In May 2008, the Winston Group and Peter D. Hart Research Associates conducted a survey of air travelers who took one or more flights in the previous year. The survey found that 33 percent of all air travelers were dissatisfied with the entire air travel system and 39 percent felt that their time was not respected in the air travel process. The survey also showed that dissatisfaction was highest among frequent travelers who flew five or more times per year. Of that group, 48 percent were dissatisfied with the air travel process and 51 percent felt that the process did not respect their time.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01262 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.894

In addition, when asked which two to three words come to mind when thinking of air travel, 40 percent of all respondents and 58 percent of frequent traveler cited the word "frustrating", while 40 percent and 32 percent, respectively, said "convenient".

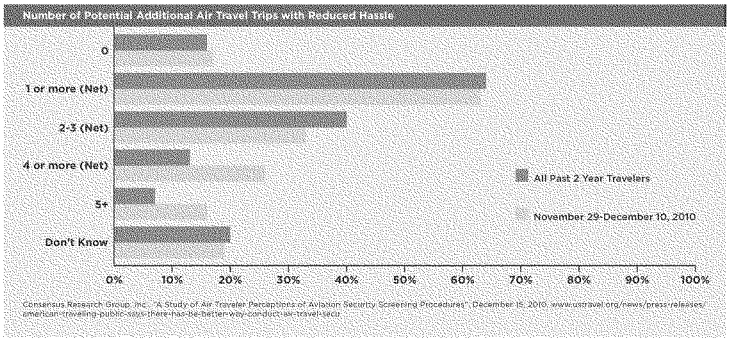
In order to identify the source of traveler frustration, the survey asked respondents to specify the area of air travel they believed to be in need of most improvement. More than one in three passengers (36 percent) chose security screening as being in most need of improvement—the second highest category among all respondents.

In fact, the 2008 survey found that the hassles of air travel were discouraging people from flying. More than one in four respondents (28 percent) said that they chose to avoid at least one trip between May 2007 and May 2008. A simple extrapolation of these results indicate that 41 million travelers, or slightly more than 100,000 per day, avoided trips during this time period. That loss of travel translates into a $26.5 billion dollar loss to the U.S. economy, including $9.4 billion to airlines, $5.6 billion to hotels, $3.1 billion to restaurants and $4.2 billion in federal, state and local tax revenue.[8]

In 2010, Consensus Research conducted a similar survey to gauge air traveler's views of the current security screening process. The survey found that perceptions of the air travel system and the resulting economic consequences are worse than in 2008 and an even larger majority of the traveling public is frustrated with the current system.

When discussing traveler frustrations, two-thirds of air travelers (66 percent) believed air travel security was a complicated problem and were frustrated by what they view to be heavy-handed procedures at airport checkpoints. The survey also found that travelers' frustration with the system was not limited to just one or two security measures but include a whole range of issues. Among the survey findings:

- Nearly 9 in 10 respondents believed that, if the U.S. can put a man on the moon, we can create a secure and efficient passenger security system that does not frighten or inconvenience travelers;
- Having to remove shoes before going through a metal detector received a higher negative response than newly implemented enhanced pat-down body searches by TSA personnel; and
- Three in four air travelers supported recruiting more professional security personnel who are trained to use personal observation, using dogs to detect contraband, and deploying sophisticated computer analyses that have proven to be effective screening techniques in the past.



Consensus Research Group, Inc., "A Study of Air Traveler Perceptions of Aviation Security Screening Procedures", December 15, 2010, www.ustravel.org/news/press-releases/american-traveling-public-says-there-has-be-better-way-conduct-air-travel-secu

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01263 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.895

Similar to the 2008 survey, Consensus Research found that the increasing frustrations with the air travel security system continue to impact when and if people choose to travel. However, the number of avoided flights has increased and now nearly two in every three air travelers (64 percent) said they would fly more if security procedures remained as effective but were less intrusive and less time-consuming. On average, the survey found that travelers would take between two and three more trips a year if the hassle could be reduced without compromising security effectiveness. These additional trips could add $84.6 billion in spending and 888,000 more jobs to our economy.

Of all the traveler sentiments polled, the 2010 survey showed that there was overwhelming agreement on a single issue—75 percent of air travelers believe that there has to be a better way to conduct aviation security in the United States.[9]

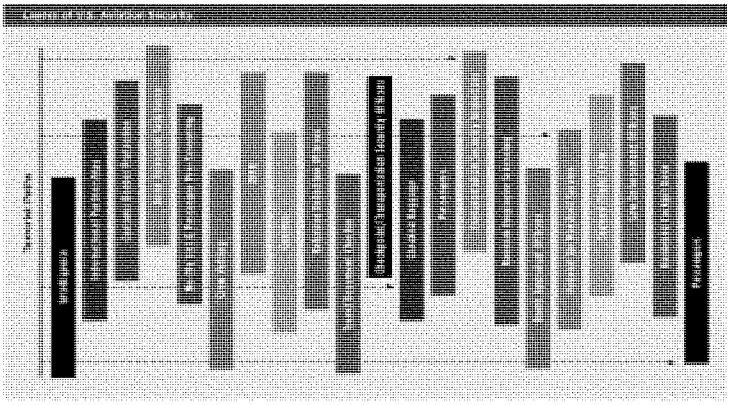
The Growing Burden of "One Size Fits All" Security

As traveler frustrations with the current system grow, the number of TSA passenger screening procedures is also expanding.

Many of the screening procedures were implemented in direct response to terrorist organizations developing new and innovative methods to carry out attacks and evade common screening practices. For example, on December 22, 2001, an al Qaeda affiliate attempted to set off explosives concealed in his sneakers, while onboard American Airlines Flight 63 from Paris to Miami. On December 25, 2009, a Nigerian citizen associated with al Qaeda concealed explosives in his underwear and attempted to ignite them onboard Northwest Airline Flight 253 from Amsterdam to Detroit. In each case, the terrorists constructed explosive devices that evaded detection at security checkpoints.

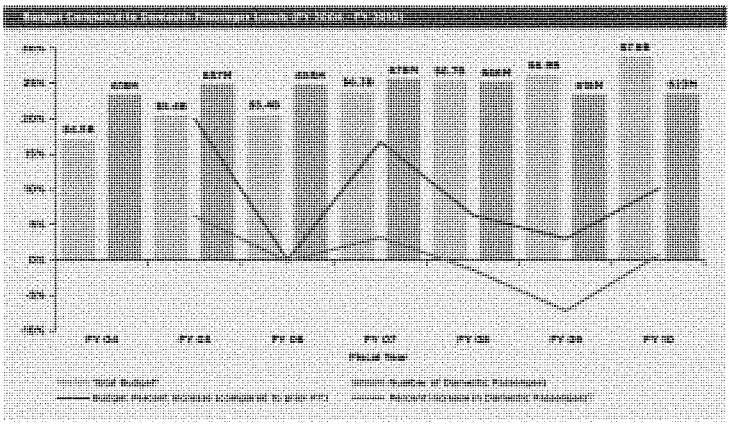
TSA responded to these types of failed attacks by adding additional procedures at passenger checkpoints. After the attempted shoe bombing in 2001, TSA required all airline passengers to remove their shoes for scanning by x-ray machines before moving through security checkpoints. Following the attempted Christmas Day bombing of 2009, Congress and TSA accelerated and expanded the deployment of advanced imaging technology (AIT) machines to most major airports throughout the U.S., and TSA implemented enhanced pat-down procedures as a form of random and secondary screening.

In 2009, a report issued by the Government Accountability Office (GAO) concluded that TSA deployed many of the new security procedures and programs without the benefit of a comprehensive risk assessment. The GAO argued that without such an assessment, TSA could not provide reasonable assurance that its limited resources were being directed at the highest priority threats in the most cost effective manner. Furthermore, GAO expressed concern that TSA implemented some security programs in response to high-profile terrorist



VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01264 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.896



events, and administration and Congressional pressure—rather than a comprehensive risk assessment.[10]

The findings of the GAO report bring into question cost and security effectiveness of adding more security procedures without employing a true risk-management strategy. Each new layer adds significant costs to maintaining the current system and places additional burdens on all aviation stakeholders. For example, by adding new screening procedures and technologies, TSA must also retrain existing employees, hire new screeners to meet increased workloads or perform new functions, and educate airports, airlines and the traveling public of the changes—all of which require vast resources. Moreover, most new technologies and procedures are deployed on a large scale—instead of on a targeted basis determined by risk—because TSA screens nearly all airline passengers using the same methods of primary screening.

Using a "one size fits all" approach for passenger screening and continually adding to the number of security procedures at each passenger checkpoint contributes to large annual increases in TSA's budget. From FY 2004 through FY 2010, TSA's annual budget increased by almost 70 percent, from $4.5 billion to $7.6 billion. In FY 2008 and FY 2009, TSA's budget increased by more than $600 million despite declines in year over year airline passenger levels. The American people might be surprised to learn that in some years, the budget of TSA was greater than that of the Federal Bureau of Investigation, which investigates cases of terrorism and handles the entire federal law enforcement agenda.

During the recent recession, declines in air travel largely masked the underlying problem at U.S. airports. The FAA, however, now predicts that yearly passenger totals will grow from 713 million domestic and international passengers in FY 2010 to nearly 1.3 billion in FY 2031. In the next five years alone, FAA predicts that passenger levels will grow by an average of 3.7 percent per year, and continue to grow at an average of 2.5 percent from FY 2016 to FY 2031.[13] With such steep rises in passenger levels, TSA will be hard pressed to control the growth of its budget, wait times at security checkpoints will increase, and the burdens of the current system will slow economic recovery unless Congress and TSA develop a long-term, risk based strategy to focus assets and resources at the highest priority threats.

As Secretary of Transportation, Ray LaHood, recently stated in reference to FAA's forecasts for passenger growth, "We need to invest in aviation today to make sure America's economy remains competitive."[14]

Moreover, as the recent attack in a Russian airport demonstrates, lines of passengers in the airport are themselves a significant security risk. Terrorists who may recognize the difficulty of penetrating the actual checkpoint may opt to

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01265 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.897

attack the aviation system and travelers before they even have a chance to be screened at the checkpoint. Former TSA Administrator Kip Hawley wrote in a recent op-ed that:

> Effective security is, in fact, risk management. Our political leaders and security authorities make judgments about where to set the risk-management needle. They have chosen to take the minimum possible risk at airport passenger checkpoints, resulting in pat-downs and plastic bags. The needle registers a little more tolerance in the maintenance area, or so-called backside of airports, and more still in the public areas. But how much risk do we want to accept in these public areas? And how much more hassle can we take?[15]

The issue of security in airport "public areas" is directly related to wait times and passenger volumes at TSA checkpoints. Since its creation, TSA set a goal to keep average wait times at passenger checkpoints below 10 minutes.[16] However, according to a 2007 GAO report, average wait times at the nation's busiest airports, which account for 75 percent of all passenger boardings, have consistently been over 10 minutes. In FY 2005, average wait times at the largest airports were 12 minutes and, in FY 2006, the average wait increased to 12.6 minutes. It is important to note that these average wait times include both peak and non-peak travel days, which balance out lengthy wait times that can exceed 40 minutes.[17]

Given the importance of passenger wait times to both security and levels of passenger frustration, it is unfortunate that, as of 2009, TSA has stopped providing information on average security checkpoint wait times to the general public. This lack of information not only inhibits passengers from adequately gauging the necessary arrival time before a flight but it also prevents independent analysis of TSA's success in reducing wait times year-over-year.

In addition, because most travelers are unwilling to risk missing flights and thus incur airline fees to change a ticket or fly "stand-by", travelers must plan for the worst-case scenario on security wait times and arrive at the airport far in advance of each flight. Many U.S. airlines advise their customers to arrive at the airport sixty (60) or seventy-five (75) minutes before the flight even if they are not checking luggage. While most passengers arriving this early will have cleared security far in advance of their flight, the "wait time" near the airport departure gate should be considered an unnecessary by-product of inconsistency at the TSA checkpoint.

International Aviation Security and Impacts on Domestic Travelers

International law and business practices deployed by governments, airlines, and airports around the world have direct impacts on the way TSA and the U.S. government fulfill their domestic responsibilities.

The case of Umar Farouk Abdulmutallab's unsuccessful attack on an in-bound international flight on Christmas Day 2009 demonstrates the linkage between international and domestic security concerns.[18] In short order, this incident generated a plethora of changes in how governments around the world, including the U.S., sought to achieve aviation security. The processes that surround a flight have changed significantly in less than fourteen months, including major acquisitions of new screening technology at U.S. airports; negotiations between U.S. authorities, international carriers, international airports, and other governments concerning screening equipment and information sharing; and changes to watchlisting protocols.[19]

As the December 25 failed bomb attack revealed, our current system—both domestic and internationally—is reactionary in nature. Within hours of the attack, TSA issued Security Directive 1544-09-06, requiring passengers to put away all carry-on baggage, blankets, pillows, and personal belongings and remain in their seats beginning one hour prior to arrival. This directive was superseded by new rules announced in early January 2010 on international screening protocols for passengers traveling from certain high-risk countries.[20] Later, on April 2, 2010, DHS Secretary Janet Napolitano announced a change in rules relating to air carriers with international flights to the U.S. These efforts subject passengers traveling to the U.S. to enhanced security measures including random screening through the check-in and boarding processes, and the use of explosive detection and advanced imaging technologies, canine teams, pat downs, and other security measures.[21]

It is also important to note that the regulation and execution of passenger screening in the U.S. is markedly different from other countries. A 2006 report produced by the Reason Foundation detailed 33 European airports that successfully outsourced their passenger and baggage screening operations to private contractors.[22] Many of these same countries continue to employ similar procedures today.

Conclusion

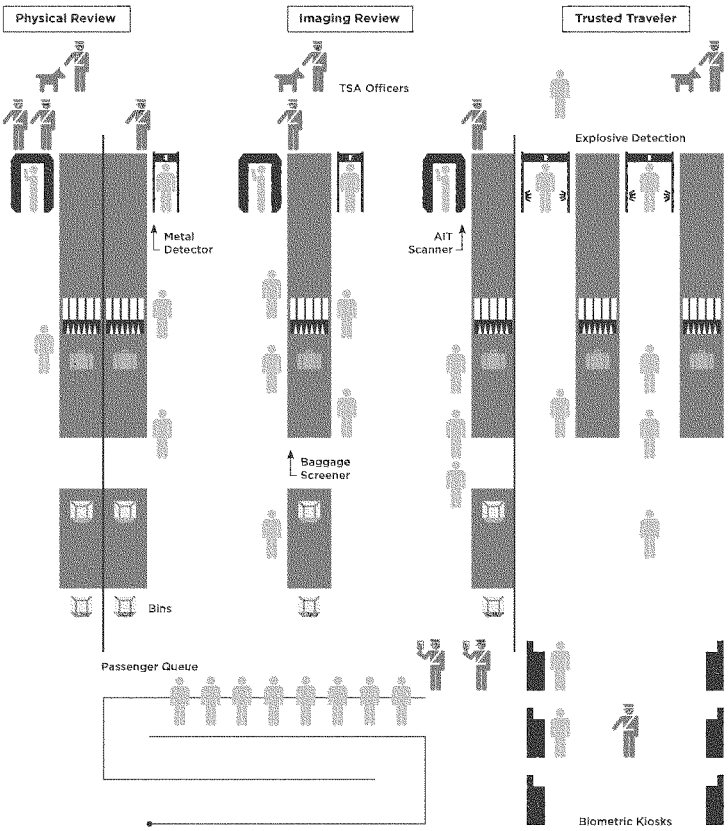
It is not hard to document public angst about airport passenger screening procedures. However, the recommendations that follow provide real and implementable solutions to these pressing problems. If implemented by Congress and the Executive Branch, these recommendations would make our aviation security system more efficient, more secure, and more in line with what an overwhelming majority of Americans want—a better way to conduct aviation security.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01266 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.898

Recommendations

VISION FOR AVIATION SECURITY



VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01267 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.899

GOAL No. 1

Improve the TSA Checkpoint by Increasing Efficiency, Decreasing Passenger Wait Times and Screening Passengers Based on Risk

"A proper multi-level security scheme would tag each traveler with a risk assessment—Low, Medium, High, Orbital—and then tailor a protocol to fit that risk assessment. More than 99% of all travelers pose little to no risk. It makes no good security sense to assign them to the "high" risk pool…"

— P.K., *YourTravelVoice.org, 11/19/2010*

Our country needs to transition from today's one-size-fits-all screening process, where travelers have no input or choices, to an environment where passengers can choose between three fundamentally different checkpoint experiences

The first is the "Trusted Traveler" program described in great detail below, which could provide a significant portion of the daily travelers in the U.S. with an alternative screening process that recognizes their low-risk status.

The second passenger choice, "Imaging Review", should utilize the most sophisticated equipment available to non-intrusively screen passengers for prohibited items and dangerous substances, with robust privacy protections built into the process.

The third experience, "Physical Review", should provide personal physical searches for passengers who prefer this approach to any sort of non-intrusive imaging or identity management. TSA would develop physical inspection regimes designed to appropriately inspect travelers who wish to travel without going through advanced imaging equipment and/or cannot provide appropriate identification assurance of their identity to TSA.

In a country of over 300 million individuals, we recognize different travelers have different priorities and different visions about their privacy expectations. Some travelers are most concerned about providing information about themselves to the government.[23] Other travelers are offended by physical searches that currently inspect sensitive areas of their body or by AIT machines that produce detailed images for review.[24] Some segments of the traveling public, such as those with medical conditions or implanted medical devices, have been very vocal in asking for a better system that would address their specialized needs. [25] While the majority of travelers, according to polls, are supportive of existing security measures,[26] TSA's screening process should be designed to meet these varied expectations without sacrificing security.

Problem

A one size fits all solution to passenger screening has blocked deployment of a Trusted Traveler program that will enhance security and increase passenger throughput.

"How about implementing a "Trusted Traveler" program, like Global Entry, that expedites the TSA screening process? Make it a strenuous background check, supported by biometric screening, and let me move on; no metal detectors, taking off shoes, or opening bags. That is a service for which I would be willing to pay." —R.M., *YourTravelVoice.org, 11/22/2010*

The Aviation and Transportation Security Act, which established TSA allowed for the creation of a voluntary trusted traveler program. Congress believed that this requirement would

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01268 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.900

be an appropriate and effective mechanism to allow TSA to focus its limited resources on high-risk travelers who deserve more security attention and spend less time on passengers identified as "trusted".[27]

Unfortunately, programs dubbed "registered traveler" (RT) never lived up to the hopes of Congressional authorizers—or the travelling public. Private sector vendors of RT programs succeeded in creating a secure, interoperable, biometrics-based identity credential that certainly helped verify the identity of the card's holder upon arrival at the airport. Aggressive marketing about shorter wait times attracted approximately 250,000 enrolled members.

However, little else emerged from the program, as TSA was unwilling to provide any security benefits (i.e. allowing card holders to keep on their shoes when walking through the metal detector) for the enrolled members of the RT program. Although applicants submitted fingerprints and iris scans as part of their application, TSA refused to compare the fingerprints against applicable criminal and terrorist databases. In 2008, TSA withdrew from the program, leaving it as an airport-supported 'front-of-the-line" only program.[28] Less than a year later, the largest RT vendor abruptly ceased operations and the network of 21 airports offering RT services collapsed.[29]

In 2010, several vendors relaunched RT operations at a handful of airports but the current program remains devoid of either a background check or changes to the security checkpoint.[30]

Solution

Implement a risk-based trusted traveler program. Congress should authorize TSA to implement a new, voluntary, government-run Trusted Traveler program that utilizes a risk-based approach to checkpoint screening, with the goal of re-focusing resources on the highest risk passengers.

> "We've been talking for years about establishing a screening system that takes risk into account. Creating a trusted traveler program is, without a doubt, one of the best ways to control the cost of aviation security and improve efficiency." —The Honorable Tom Ridge

The failure to date of the RT program is unfortunate but also perhaps appropriate because it does not utilize risk management by changing the checkpoint process for enrolled members who demonstrated and confirmed their low-risk nature. It is time for a true risk management trusted traveler program—which should help TSA and airport authorities better manage aviation security and checkpoint resources while also enhancing the passenger experience for all travelers.

TSA Administrator John Pistole is signaling a new willingness to implement a risk-based program at TSA. In recent remarks, Administrator Pistole commented that TSA was looking to facilitate:

> those individuals who are willing to provide more information about themselves in exchange for a different level of screening. So it's more of an identity-based screening than physical screening … there's groups of people out there, the very frequent travelers, who are willing to provide more information. We're looking at what we can do as a government, providing what will probably be a fee-based service, but to say 'you don't want to stand in line, here's what we're going to do'.[31]

Creating a new Trusted Traveler (TT) program that utilizes true risk-management requires a tightly-controlled enrollment and re-verification process, a confirmation process at the airport that ensures only enrolled individuals are utilizing the TT screening lanes and a checkpoint process that reflects the low-risk nature of the traveler. All three elements are required, and all three are achievable in 2011.

Enrollment

In time, enrollment in such a voluntary program should be open to all Americans, but TSA should focus initially on certain populations of extreme low-risk passengers. For example, many individuals are already part of previously federally-vetted populations and already have been deemed by our government as worthy of trust to very sensitive facilities, information, or law enforcement authorities. These individuals should be offered free enrollment in this new TT program to help speed equipment deployment and public understanding of the program. Specific populations include:

1. Current members of Customs and Border Protection Trusted Traveler Programs, including Global Entry, SENTRI, NEXUS; and the FAST Commercial Driver ID Card;
2. Holders of a valid TSA Transportation Worker Identification Credential (TWIC);
3. Any federal government employee, member of the armed forces, or Federal contractor with an active Security Clearance at Secret-level or above and without an overdue periodic reinvestigation;

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01269 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.901

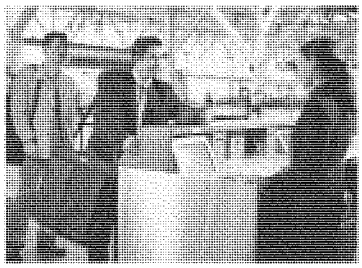
4 | Active federal law enforcement officers (U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, the Federal Bureau of Investigation, U.S. Secret Service, the Drug Enforcement Agency, Federal Air Marshals, etc); and
5 | Airport workers who are active participants in SIDA program, which allows unescorted access to secure areas of an airport.

Following this initial enrollment, TSA should develop and issue regulations to expand enrollment to qualified members of the general public. In order to provide a reasonable cost-per-flight and to generate workforce efficiency for TSA, the expansion should be targeted to travelers who fly frequently. Applicants should first be required to possess the following attributes and would be offered enrollment for a fee commensurate to cover the cost of the program:

1 | Must not be on no-fly or selectee list managed by TSA;
2 | Must hold a current U.S. passport, passport card, enhanced driver's license, or license issued by a state that is compliant with the REAL ID statute;
3 | Must meet TSA criteria on the amount of flights flown or be sponsored by a US airline due to his/her participation in the airline's frequent flyer program;
4 | Must have undergone a fingerprint-based Criminal History Records Check that does not disclose that he or she has a disqualifying criminal offense;
5 | Must be confirmed as having no outstanding wants or warrants for disqualifying criminal offenses or outstanding tax payments;
6 | Must not have been refused enrollment in a CBP Trusted Traveler program; and
7 | Must have identity confirmed via a name-based review of publicly-available commercial information conducted by TSA under new authorization from Congress.

In terms of disqualifying criminal offenses, the existing federal program which governs individuals who can have access to defined secure areas of an airport—the Secure Identification Display Area (SIDA)—sets out an effective list, and should be adopted in its entirety. Under SIDA—and therefore under this trusted traveler vision—an individual is disqualified if convicted or found not guilty of by reason of insanity, of any disqualifying criminal offenses—usually serious felonies or transportation-related crimes—in any jurisdiction during the 10 years before the date of the individual's application.[32]

This program would require Congress to authorize TSA to utilize publically-available commercial data to assess the risk



profile of TT applicants. That authorization should take place as soon as possible in order for TSA to begin assessing the value of this data as part of a web of information that would help determine a traveler's risk—and therefore a passenger's "trusted traveler" status.

TSA should control the enrollment process for the TT program, including developing an application infrastructure, collecting biometric information from applicants, and conducting the required checks against criminal and other databases to identify inappropriate applicants. TSA should be authorized to utilize private sector expertise for program marketing, card construction and personalization, and database management. For applicants, upon successful enrollment, the applicant would be mailed a secure identity document containing digitized biographical and biometric information, readable biographic information, and a digital photo.

Verification

In the Trusted Traveler program, upon reaching the lead position in a separate security line for TT enrollees, the traveler would enter a kiosk area designed for one traveler. The traveler would present a biometric (fingerprint, iris, etc.) to a TSA-managed biometric collection device. The presentation of the biometric would trigger a real-time match of the individual's identity against a database of trusted travelers, confirming prior enrollment and checking that the trusted status has not been revoked since enrollment.

The kiosk would next direct the traveler to present a boarding pass. The name on the boarding pass would be read by the kiosk and matched against the name of the individual tied to the biometric presented. During the implementation phase, TSA should coordinate with airlines to have their passenger name record systems denote boarding passes with a indicator that the passenger is enrolled in the TT program.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01270 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.902

The kiosk would be programmed to randomly designate a very small percentage of enrolled travelers for a normal physical screening review. The TSO manning the TT area would direct such randomly-selected travelers to the front of the traditional TSA checkpoint line for the same physical review deployed for at that particular checkpoint for non-TT enrollees.

Trusted Traveler Screening

If the traveler's biometric identity has been confirmed as eligible for trusted traveler status and the boarding pass is confirmed as tied to the same traveler, the traveler would walk through an explosives detection portal to determine the presence of explosives. The traveler would pass through the machine without divesting personal items in pockets and would leave external garments and shoes on. Separately, the traveler's carry-on bag(s) (if any) would also go through an explosives detection scan. TT enrollees should still be prohibited from carrying certain dangerous items aboard an aircraft and TSA should determine the correct calibration of the scanning equipment to detect these items.

If neither the traveler nor his/her carry-on bag(s) set off an alarm based on the presence of explosives, the passenger would proceed to the gate area.

Security Enhancements to Further Secure the Trusted Traveler Lanes

Several critical capabilities are required for the success of this program. First is the technology mentioned above—it must be developed, tested and able to be widely deployed in the commercial aviation environment. During 2010, TSA deployed explosives detection equipment but numerous airports still do not have such equipment and independent reviews of the effectiveness of the equipment are underway by GAO.

The second capability needed is a better trained TSA workforce. While a Trusted Traveler program can help TSA dedicate fewer TSO resources to checkpoints designated for those travelers, TSA should use this program as a tool to begin creating a more professional and capable workforce with a set of skills that help deter and detect terrorists. To create more professional TSOs, TSA should deploy a robust training program—akin to the FBI's Academy—that focuses on continually building new sets of skills and talents within this workforce. TSOs would, for example, need training in areas including critical thinking, ability to demonstrate a "professional presence", strong communication skills, thorough understanding of the terrorist mindset, an effective understanding of how to interpret intelligence information, and enhanced training in team dynamics.

With this training, TSOs in designed TT lanes would be able to help passengers use the kiosk and screening equipment mentioned above, while also being better trained to ensure that any traveler who is not confirmed for eligible TT travel or is selected for random screening is effectively removed from the TT area.

TT lanes should also possess an appropriate Behavioral Detection Officer (BDO) capability, working to detect any behavior that is outside the norm for a trusted traveler.

Finally, TSA should maintain an appropriate canine team trained to detect explosives or other substances which might compromise the safety of the aircraft in and around the TT area.

This combination of checkpoint assets—technology, better trained TSOs, capable BDOs, and canine teams—would create the in-airport infrastructure for a TT program that effectively removes low-risk travelers from the one-size-fits-all solution in airports today, while also allowing TSA to deploy greater resources at checkpoints that assess non-trusted travelers.

The goal of a fully-deployed TT program should be to process at least 25 percent of passenger trips while using far less than 25 percent of TSA's existing screening budget.

Problem

The airports, airlines, and TSA all have some control over the security checkpoint—leading to inefficient uses of space and added confusion for travelers.

Traveler confusion over security starts from the moment he or she enters the security queue because travelers do not know whether the security process is controlled by the airport, airlines or TSA.

Many travelers are not sure who controls the security lines in front of the actual TSA travel document checker. Numerous Blue Ribbon Panel members noted that airports and TSA are inconsistent in how they divide responsibilities and how that division is communicated to the travelers.

While this issue may not top the list of items that offend travelers, it reflects a broader issue of confusion about the commercial aviation security process, and which parties bear what level of responsibility for the status quo. When trying to have questions answered about a particular security procedure, travelers often are told by TSA, airports, and airlines that confusing and inconsistent rules are not their responsibility at that particular airport. Additionally, confusion and unclear responsibilities make it difficult for stakeholders to push for change.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01271 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.903

Additionally, because TSA is restricted in the amount of floor space it controls at each airport, the agency is often unable to design the most efficient layout for security checkpoints that can adequately handle each airport's passenger loads. Without adequate control over floor space at security checkpoints, TSA can be forced into smaller areas because airports and airlines have a strong interest in controlling as much airport space as possible to allow for more profit generating services such as vendors or screening lanes for loyalty customers. Several airlines have built business models on this confusion by offering preferred security lines to their customers paying a surcharge for a particular flight or those at a certain level in the airline's frequent flyer program.[35]

Solution

Give TSA authority over entire checkpoint area. Congress should immediately act to clear up confusion over "ownership" of commercial aviation security and authorize TSA to control the entire security checkpoint starting at the beginning of the security lines and ending after a traveler exits the screening area.

> "For airport authorities, vendors and airlines, control of airport space impacts their bottom lines. For TSA, control of airport space impacts checkpoint efficiency and security. If we're going to hold TSA accountable for improving checkpoint efficiency and security then the agency needs the proper control and operational flexibility to do so." —The Honorable Kathryn "Kitty" Higgins

By taking this step, all stakeholders in the commercial aviation security process will understand who is in charge of security, and what entity is responsible for making changes to improve the security screening system. It should be simple: TSA controls security, and should be responsible for making it work better, with the support of all travel stakeholders—airlines, airports and passengers. Security lanes should be organized to most efficiently screen large numbers of travelers based on their actual risk, not based on their loyalty to a particular airline or the price of a single ticket.

By separating out profit incentives for particular stakeholders in the aviation system and allowing security operations to be constructed without profit calculations, TSA will be able to best utilize its limited resources and space to create lines and deploy equipment to manage traffic. For instance, in large airports, TSA might be able to deploy a full complement of screening options—Trusted Traveler, Imaging Review and Physical Review—if it had the flexibility to use the entire space devoted to screening. TSA could also utilize better industrial engineering practices that increase efficiency, such as constructing larger passenger divestiture areas or installing automatic bin returns.

Problem

Too many travelers enter the checkpoint unaware of the security screening process and fail to live up to their responsibilities to make the system work smoothly.

> "I think a major problem is when people are unprepared and not paying attention to the MANY simple audio and visual reminders that the TSA provides. No one likes to be searched or delayed, but if there were some additional way to "prep" travelers on the basics of 3-1-1 and what to take off, put in bins, on belts and in the trash it might further reduce aggravation for everyone." —R.C., *YourTravelVoice.org, 11/18/2010*

An important part of a smoothly operating security checkpoint is an educated traveler. Travelers play a critical role in making the system operate smoothly, from packing their bags in a manner that facilities screening, to following checkpoint procedures, and treating TSA and aviation employees with respect and courtesy.

In a chaotic system processing millions of travelers each day, security lines can be delayed for any number of reasons—from a traveler leaving a laptop in a bag or failing to take off a belt with a heavy metal buckle to a family trying to navigate a checkpoint with children and strollers. In the most egregious cases, TSA must deal with the occasional traveler who demonstrates clueless ness about the current security environment by bringing items like chainsaws and machetes into the airport.[33]

On the government side, TSA has worked hard to increase communication with travelers. For example, the agency launched a mobile "app" for travelers on the go to learn more about security screening. The TSA.gov website has a dedicated "Travelers" section, in addition to a "What to Know Before You Go" segment on the front page of the site. Like most consumer oriented businesses, TSA has a blog, http://blog.tsa.gov/, focused on answering passenger questions and offering up information on important travel issues in an informal manner.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01272 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.904

Yet despite all of this public education effort, some passengers remain woefully unprepared when they arrive at the checkpoint. This ignorance has several negative effects. First, it creates a bad experience for passengers by slowing down screening. Second, this situation forces TSA officers to help passengers comply with rules, as opposed to focusing on identifying possible threats at the checkpoint.

Solution

Improve preparation of travelers. **Industry stakeholders should work with TSA to improve their education and communication on security rules and regulations, targeting locations and sources that travelers are likely to review as they book or prepare for the trip.**

> "An educated traveler is an effective traveler. Those companies with rich relationships with their customers need to develop deep relationships with TSA to make sure we educate our customers on what security means for them. From the time they pack their bag to their arrival at the airport to their compliance with rules on liquids and laptops, travelers need to play their part to make the system flow smoothly." —Mr. Sam Gilliland

Most travelers are not likely to go to the TSA website in advance of their trip. Thus TSA's tools to educate passengers on what to expect when at the security checkpoint need to be reinforced by the private sector—specifically, by those companies who sell travel or travel related services to a commercial aviation passenger.

For example, when a traveler buys a ticket to fly, the party from whom travel is bought (directly from the airline, from an online travel site, or from a travel agent) generally sends the passenger an email confirming the flight, departure and arrival times, and related information. This communication should also include basic information about passenger screening requirements, while directing the traveler to the "Traveler" segment of the TSA website.

Additionally, any travel reminders, including the reminder to check-in online, should include information on travel security procedures while also directing the traveler to the TSA website.

Other companies often involved in a trip also have the opportunity to make their customer's experience at TSA more pleasant by communicating security requirements. Passengers who reserve hotel rooms, car services, or rental cars generally get confirmations, either in writing or electronically, from these entities. Again, basic checkpoint security information should be included on any electronic or written information going to a customer who is using a service before or after a commercial aviation flight. Many travel providers currently advise travelers to go the TSA website but including relevant information and new procedures in their own communications will influence travelers who may be unlikely to click through to the TSA site.

One of the most obvious locations where travelers can be directed to TSA information is through websites where individuals manage frequent flyer or frequent customer accounts. Including easy-to-find banners or boxes on TSA security procedures would certainly help spread information about what an air traveler should expect.

All of these examples should become best practice tools for companies in the travel community. By enhancing a customer's understanding of the TSA security experience, these companies would help travelers become more informed and, hopefully, decrease the number of unaware passengers at security checkpoints. In sum, prominently adding TSA travel tips to any electronic or written documentation a traveler takes on a trip should become a "best practice" throughout the travel community, and will over time contribute to a smoother checkpoint.

The Aviation Security Advisory Committee, when reconvened, might also consider whether it would be helpful to TSA's mission to allow TSA to reinforce security compliance by penalizing travelers who fail to abide by normal guidelines by having them restart their security review, or whether such a step would be too disruptive to the queuing function.

Problem

In order to avoid paying baggage fees, passengers are bringing more carry-on bags onto each flight, which increases checkpoint congestion and requires TSA to devote more resources, equipment and personal to screen in-line passenger bags.

> "I believe the government should put a stop to the airline bag policy and minimize carry-ons for both our safety and speed of travel. Perhaps TSA could also offer an express line for people with one or less carry-ons?" —R.B., *YourTravelVoice.org, 11/20/20*

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01273 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.905

In recent years, most airlines began charging fees for checking baggage.[34] Part of the current congestion and checkpoint inefficiency is created by passengers carrying on luggage that they would otherwise check but do not, either because they want to avoid the baggage fee, or because they do not want to wait at the luggage carousel for a checked bag to arrive. Since commercial airlines began charging fees for checked baggage, the number of carry-on bags per flight has increased and the number of checked bags has decreased, forcing the checkpoint process to handle more and more luggage. On March 2, 2011, at a hearing held by the U.S. Senate Committee on Appropriations, Secretary of Homeland Security Janet Napolitano testified that the extra carry-on baggage as a result of the checked baggage fees caused roughly $260 million in increased costs to TSA.[35]

This higher volume of carry-on bags leads to longer wait times in the passenger screening lines due to baggage congestion and increased alarms caused by passengers intentionally or unintentionally packing prohibited items in their carry-on bags. Increased carry-on bags also cause TSOs to focus more resources on screening carry-on bags, and less time looking for passenger threats.[36]

Solution

Encourage fewer carry-on bags. The DOT should issue regulations requiring airlines to allow passengers one checked bag as part of their base airfare and standardizing existing rules covering the quantity and size of items that can be carried onto the airplane.

> "Today, the practice of allowing airlines to charge for checked baggage gives travelers a strong economic incentive to carry as much as possible onto their flights. While these fees help airlines improve their bottom lines, they also result in more congestion and delays at security checkpoints. This increase in congestion actually decreases security while adding significant costs to the taxpayer. It's time to rethink those fees and allow one bag per passenger to be checked without charge."
> —The Honorable Kathryn "Kitty" Higgins

In order to mitigate the economic incentive many airlines create for passengers to carry more bags onto an airplane, the Department of Transportation (DOT) should issue regulations requiring airlines to allow each passenger to check one bag—similar to the normal weight and size of a carry-on bag within the base airline ticket fare and free of additional charge, should the traveler choose to do so. Airlines would be free to impose charges for additional or oversized bags, should they choose to impose them.

Furthermore, DOT should set a standard for the number and size of items that a passenger may carry onboard a commercial aircraft. Today, each airline has its own rules and equipment governing what customers can carry on and this creates confusion—and frustration—in the travel community. Whether a bag is eligible to be carried on should not be dependent on the particular aircraft or airline. With a DOT standard in place, airlines would be charged with enforcing these standards, and travelers would have consistent criteria for deciding of whether to carry-on or check their bags.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01274 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.906

GOAL No. 2

Governmental Efficiency and Cooperation in the Execution of its Security Responsibilities

"We shouldn't just give our people a government that's more affordable. We should give them a government that's more competent and more efficient. We can't win the future with a government of the past…In the coming months, my administration will develop a proposal to merge, consolidate, and reorganize the federal government in a way that best serves the goal of a more competitive America. I will submit that proposal to Congress for a vote—and we will push to get it passed."

President Barack Obama, *2011 State of the Union*[37]

Many of the obstacles hindering more effective solutions to our aviation security challenges are due to outdated government organization charts and the current division of responsibilities between federal agencies, airports, airlines, and the private sector. It is time to review old paradigms and look for solutions beyond those that TSA can fix by improving checkpoint operations.

Problem

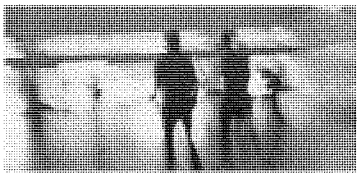
The current Security Partnership Program allowing airports to utilize private sector security screeners is ineffective and gives private firms little flexibility to change or improve the screening process.

As part of the Aviation and Transportation Security Act of 2001, Congress included a provision that allowed airports to "opt out" of the federal screening workforce. In response to this requirement, TSA created the Screening Partnership Program (SPP), under which airports can apply to have qualified federal contractors conduct checkpoint screening, under TSA oversight and a TSA contract.

To date, only a limited number of SPP companies are taking over passenger screening at a handful of airports. Many of the airports utilizing the SPP report that operations have been effective. However, the number of airports opting to join the SPP is smaller than expected. In part, this is because airports are severely limited in what parts of the screening process can adjust under their arrangements with TSA. As the GAO found in a 2009 report:

> With regard to the SPP, … TSA and its private screening contractors are constrained by both law and TSA policy, which limits opportunities to make programmatic changes to improve contractor performance and achieve cost savings. Therefore, it is understandable that differences in performance and costs of SPP and non-SPP airports may not vary considerably.[38]

This lack of flexibility may be one reason that TSA recently announced it will no longer consider new applications for airports to utilize private sector screeners. According to Administrator Pistole, after evaluating the SPP, he did not "see any clear or substantial advantage" to the SPP option.[39]



VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01275 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.907

This announcement, coupled with a recent decision to provide certain collective bargaining rights to TSA employees,[40] sparked a robust debate whether TSA should only assume a regulatory role or continue using a large federal workforce executing day-to-day operations at hundreds of domestic airports.[41]

Solution

Empower airports and the private sector to innovate and improve security. Congress should overhaul the TSA Screening Partnership Program so that it becomes a viable, flexible and innovative option for helping airports deploy more efficient and effective security solutions that are tailored to their specific requirements.

"TSA is clearly in charge of setting standards for aviation screening. However, particular airports should have the flexibility to utilize innovative private sector methods to increase efficiency and customer satisfaction, while maintaining security. In an era of enormous budget deficits, Congress needs to revamp the SPP to better achieve these goals." —The Honorable Jim Turner

The positive experience of current SPP airports indicates the value of the program, but it is clear that airports must be given more flexibility to match their workforce considerations with the security needs of their facility. With the current debate over unionization underway, it is important to point out that airports utilizing the SPP option may choose to engage a unionized workforce, depending on their local needs and laws.

In order to improve the SPP and expand the universe of airports using a qualified contractor, TSA-contracted and regulated contractor, TSA should publicly acknowledge the statutory basis for the Screening Partnership Program and announce its support for a revitalized SPP as an option for airports.

Congress, working with TSA and airports, should enact legislation to reform the SPP and stimulate use among the airport community. New elements of the SPP should include the following:

- As part of the checkpoint requirements development process, TSA should provide airports and checkpoint operators (public or private) with performance metrics of the 20 largest airports in the country. TSA should then solicit comments from private contractors on how checkpoint operations can be improved at those airports; Congress should specifically authorize SPP airports to shift resources between threats in the airport environment, to utilize airport-specific lane management tools, to execute multi-year equipment purchases, and to include customer service criteria in employee evaluations; and
- TSA should issue a fixed timeline and publically-stated criteria for considering SPP applications, to fix a problem with the prior program that left airports without a decision on their applications for far too long.

In addition, Congress should request that an independent entity, such as the GAO, examine whether having TSA serve both as regulator of aviation security and as the executing agency for most services, is a more effective model than having TSA provide top-down oversight and regulatory authority over security officers hired and managed by airports.

Problem

Today's public policy and regulatory dialogues on aviation security issues are largely conducted by TSA, airlines and airports, with travelers excluded from the debate.

"The TSA is another good example of inefficient run operations. A private organization would have hired efficiency experts to monitor the waste. Here is an example: each airport sets up these tables and trays to put items in as they pass through the x-ray machines. They hire people to continuously return the trays manually from the end of the line back to the beginning. They can't seem to figure out that it would be far more efficient to have a roller conveyor automatically return the trays to the beginning." —P.B., *YourTravelVoice.org, 11/20/2010*

For almost two decades, the FAA and then TSA operated an Aviation Security Advisory Council (ASAC) that engaged a wide array of interested stakeholders in a dialogue on aviation security issues and policies. The ASAC members took the time to consider and learn difficult and technological issues and made meaningful recommendations to the FAA and then to TSA. Unfortunately, TSA has not convened even a single meeting of this federal advisory council since 2006, cutting off a valuable tool for TSA to engage a broader range of stakeholders than just airlines and airports.[42]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01276 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.908

This exclusion from policy-making is at odds with the Obama Administration's public commitment to increase transparency in government. As noted by the President in an executive order issued on his first full day in office:

> My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government....
>
> ***Government should be participatory.*** Public engagement enhances the Government's effectiveness and improves the quality of its decisions. ... Executive departments and agencies should offer Americans increased opportunities to participate in policymaking and to provide their Government with the benefits of their collective expertise and information....
>
> ***Government should be collaborative.*** Collaboration actively engages Americans in the work of their Government. Executive departments and agencies should use innovative tools, methods, and systems to cooperate among themselves, across all levels of Government, and with nonprofit organizations, businesses, and individuals in the private sector. ...[43]

Solution

Reinstitute the Aviation Security Advisory Committee. DHS should immediately reinstate and appoint the Aviation Security Advisory Committee to provide effective private sector input to DHS on aviation security within 180 days. DHS should also convene airport-specific working groups to identify and resolve problems affecting travelers at particular locations.

> "The traveling public is a vital stakeholder in the aviation industry. So it makes perfect sense for DHS to reach out to them through measures like the Aviation Security Advisory Committee and airport-specific working groups." —Mr. Rick "Ozzie" Nelson

TSA and DHS should immediately begin soliciting ASAC membership from airports, airlines, and representatives of the commercial aviation passenger community. Simultaneously, TSA should evaluate other communities of stakeholders who would be valuable contributors to this federal advisory council (technology vendors, academics with backgrounds studying terrorism, and risk management practitioners, for example), and issue a notice in the Federal Register within 90 days outlining the exact criteria for ASAC applicants who can advise DHS on the full breadth of aviation security issues facing the department. Following appointment of ASAC members, the ASAC should be fully functional and meeting again later in 2011.

This advisory council model should also grow to communities outside of Washington, DC—namely, to the top 20 busiest airports in the country, based on Federal Aviation Administration enplanement statistics. By convening a cross-section of stakeholders including airports, airlines, passengers and federal government officials, airport-specific solutions to aviation security can be discussed and deployed on a trial basis.

These airport-specific groups should begin their work by looking at five key issues that can help improve aviation checkpoint security. Issues for consideration include:

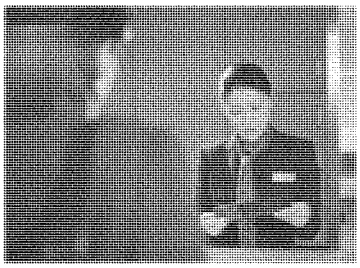
1. Establishing standards on how much space within the airport is needed to conduct effective and smooth security checkpoint operations;
2. Reviewing TSA checkpoint staffing models to assure smooth operations during peak travel times, and highlighting any federal, state or local laws or regulations that inhibit staffing changes;
3. Considering any other operational changes desired by airports, airlines, passengers or federal government officials which are consistent with and supportive of the airport's overall risk management strategy and approach, including possible use of an improved Screening Partnership Program;
4. Piloting new technologies or solutions that may improve the passenger experience at particular airports; and
5. Employing effective signage, videos, and other in-airport communications that can take advantage of the time travelers spend in the security lines to explain security procedures.

Problem

By requiring the TSA Administrator to be a presidential appointee needing Senate confirmation, the agency is subjected to leadership changes that are too partisan, too frequent, and too disruptive to the mission of the agency.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01277 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.909



Since the creation of TSA in 2001, Congress and the Executive Branch treated the nominations for TSA Administrator as normal presidential nominations subject to Congressional confirmation. Unfortunately these nominations created significant partisan division, often resulting in failed confirmations, and creating an environment where TSA Administrators serve only several years at a time.

In less than a decade, TSA had five confirmed administrators and one long-term acting administrator who served while two other TSA nominees ended up withdrawing their nominations during the confirmation process.

The difficulty of finding appropriate candidates that demonstrate a mix of law enforcement experience and an understanding of complex transportation issues is compounded by the fact that multiple Senate committees claim jurisdiction over TSA.[44]

Solution

Facilitate non-partisan leadership of TSA. The TSA Administrator should be converted to a five-year position extending across presidential administrations and filled by a non-partisan official with expertise in both security and facilitation.

"The TSA position is too important to be handled with the normal delays and partisanship that surround presidential nominations. This agency needs long-term leadership buffeted from partisan sniping, and converting it to an FBI-style long-term appointment would provide that stability." —Ms. Jessica Herrera-Flanigan

The FBI Director, being a very significant post within the larger Department of Justice, is an excellent corollary to the post of TSA Administrator. The FBI Director, however, is a ten-year appointment that extends across presidential administrations and is normally occupied by a non-political individual with demonstrated law enforcement and management expertise.

TSA would be well-served by having a similar non-partisan agency lead who could serve without regard for partisan infighting and for a significant duration to bring continuity to agency goals and investments.

A longer term of office would likely make the TSA Administrator post more attractive and result in significantly more continuity at the end of presidential administrations. During the recent transition after the 2008 Presidential election, for instance, it took a year and a half for the Senate to confirm a TSA Administrator.

Problem

TSA often deploys new technologies because of current events, not because of a thoughtful, long-term development strategy that is based on managing risk gleaned from a strong intelligence gathering and analysis capability.

TSA often deploys technology or new tools based on current events or Congressional pressure. As a result, technology vendors are forced to play "threat roulette", guessing where to make long-term investments in the development of technologies because there is no long-term vision from TSA to guide them. Unlike Department of Defense contractors, aviation security vendors are not able to rely on a long-term plan from TSA to guide their research and development and programs may be scrapped due to a shift in short-term priorities.

Unfortunately, this approach does not allow vendors to make strategic decisions with the needs of the customer (TSA) in mind, and dissuades technology and services vendors from investing even more capital in better understanding how customers would react to TSA's desired technology. As a result, the market for aviation security equipment is not as productive as it should be in generating long-term improvements in our screening technology.[45]

Companies investing in this type of market also find the TSA procurement process to be unnecessarily slow, and cumbersome and also difficult to penetrate by non-incumbents. This environment has international implications for U.S.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01278 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.910

businesses as other countries are looking to TSA for guidance on acceptable security technology to deploy.

The market for constructing cutting-edge security equipment is a growth market, and, just as with our military equipment industrial base, it is essential that domestic U.S. companies be able to compete in a worldwide market to create jobs at home and ensure our transportation systems have access to the best technology.

Solution

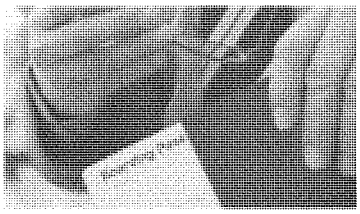
Develop a comprehensive technology procurement strategy. **TSA, in collaboration with technology vendors and the travel community, should develop a comprehensive strategy for implementing necessary checkpoint technology capabilities. Congress should provide multi-year funding plans for TSA to execute this strategy.**

> "In order to make the most efficient use of industry's investments in security technology, the TSA, vendors and travel stakeholders should work collaboratively to develop long term technology deployment strategies. These strategies must accommodate both projected threats scenarios and operational requirements while enabling an enhanced traveler experience." —Mr. Thomas Ripp

TSA should aim to develop and field technology that fits within the organization's overall risk management approach. The airport, airline and travel communities should all be part of a public-private dialogue with TSA on all such technologies with the goal of having all stakeholders well educated on the risks these technologies are designed to mitigate. While TSA need not reach total consensus among these stakeholders on the technology or tools it wants to deploy, there must be a common agreement on the risk the technology is trying to address, and its ability to do so in the operational environment. DHS should also develop mechanisms for approving technology that is successfully utilized by allies and can be rolled out in the U.S. in an effective and efficient manner.

In particular, DHS should develop mechanisms for the sharing of Research, Development, Test & Evaluation results of explosives detection technology that will expedite refreshing of technology equipment and deployment to meet emerging threats and improve passenger travel.

There are a number of technology capabilities that would make the process more secure and convenient for commercial



aviation consumers. Those improvements include technologies that would allow a traveler to keep his or her shoes on and that would allow a passenger to go through security wearing external garments and carrying non-metallic personal items. They address two of the most irritating security checkpoint issues facing commercial aviation travelers, and should therefore be at the top of the list of capabilities that would enhance the experience of a traveler.

The treatment of laptop computers and similar devices at the checkpoint is particularly important to travelers. Since 2007, TSA requires laptops to be removed from bags and screened separately and approves a certain number of "laptop-friendly" carry cases that may be screened with the laptop still inside.[46] However, the number of laptops which are stolen or broken during the screening process remains quite large.[47] As the types of electronic equipment carried by millions of travelers continues to expand to IPad's and other tablet devices, gaming equipment, and E-reader devices, confusion over TSA procedures is likely to grow.[48]

Lastly, DHS and the Department of Commerce should provide export assistance to companies selling innovative technology to foreign airports and other customers to create economic opportunity in the U.S., enhance security of foreign air travel, and ensure that the U.S. has a cutting-edge industrial base.

Problem

Many government-issued identity documents are too insecure to provide front-line security officials with a level of confidence needed to give travelers a "trusted" status.

One of the most difficult debates since 9/11 revolves around the concept of secure identification documents that would help governments identify the true identity of a traveler. The

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01279 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.911

U.S. has a long history of suspicion about a national identification card, and current federal law forbids DHS from developing such a card.[49]

However, the inability of a front-line government officer, such as TSA's Travel Document Checker (TDC), to rely on the validity of a government-issued identification has significant real-world impacts. TDC's inspect each identity document to see if it has been forged, a step that could be made much easier if only high-quality identity documents had been issued. The U.S. passport is deemed extremely difficult to forge and could be proof of identity but less than half of U.S. citizens have a passport or passport card. A federal law requiring TSA to accept state-issued identity documents for purposes of domestic air travel[46] sparked a major fight between the federal government and states concerned about costs, privacy and federalism.[50]

All stakeholders—TSA, airlines, airports and travelers—would benefit if more travelers had better identity documents. Current practices that allow a significant percentage of passengers to utilize sub-standard documents results in our government being unable to build security around identity, and instead rely on more expensive and intrusive physical screening.[51]

Solution

Encourage wider use of secure identification documents. The federal and state governments should embrace programs that build and deploy secure identification documents in order to provide higher-quality identity documents to the traveling public that meet government security requirements.

> "The 9/11 Commission appropriately noted identity management as a weakness in U.S. counterterrorism efforts. By encouraging travelers to obtain secure documentation, such as passports, the U.S. government can rely less on expensive and vulnerable physical screening regimes and more on tailored risk management tools that help identify potential terrorism suspects." —Mr. Thomas Ripp

Congress should encourage U.S. citizens to obtain U.S. passports, passport cards, and secure state-issued identity documents with appropriate tax credits to pay for federal documents and appropriate funding for states to comply with federally-mandated programs.

Moreover, through the Trusted Traveler program proposed in this report, TSA should make use of the current generation of biometric identification cards used by other registered traveler programs. Proliferation of voluntary, secure, biometrics-based IDs is a positive step for security and can serve as a platform for a wide range of benefits today and in the future.

Problem

Travelers to the U.S. with domestic connections must undergo two separate physical screening processes.

When international travelers arrive in the U.S., they are screened in the country in which their flight originated, consistent with U.S. requirements. Upon landing in the U.S., they must gather their luggage, go through customs, be rescreened and have their luggage rescreened by TSA for their continuing travel. This effort is duplicative, time-consuming, and results in a traveling experience that is frustrating to travelers.

In certain airports that serve as gateways to the U.S., the rescreening of international passengers can generate significant delays and crowding in airports as they and their large amounts of luggage mix into lines of domestic passengers.[52] As the U.S. demands that foreign governments improve their out-bound screening of passengers and baggage, it must adjust its policy of not differentiating between passengers that have arrived from countries with high-quality security standards and those who come from riskier locations.

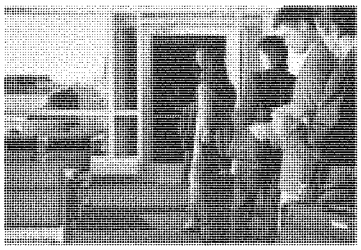
Solution

Reduce duplicative TSA screening for international arrivals. DHS should enable certain low-risk passengers who are traveling to another domestic airport to forego checked baggage and passenger screening upon landing in the U.S.

> "An easy way to improve aviation security is to weed out duplicative processes that unnecessarily hassle passengers. For example, foreign visitors that clear Customs in one airport and then travel to another U.S. destination are screened once by CBP and once by TSA. Not only is this unnecessary, but it dissuades visitors from coming to the U.S." —Mr. Bob Crandall

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01280 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.912



In order to encourage achievement of international standards and mutual recognition of comparable screening regimes that will increase security and eliminate unnecessary duplication within the international travel system, DHS, working with industry, should enable certain low-risk passengers who are traveling to another domestic airport to forego checked baggage and passenger screening upon landing in the U.S.

CBP, TSA, and a willing airline participant should pilot a procedure that would avoid rescreening of inbound international checked baggage for certain continuing passengers. Global Entry participants who have nothing to declare, who have not been to countries of concern, and who are continuing to another domestic airport may be an appropriate population for this pilot.

For longer term solutions, TSA should work with the airlines for developing a system to tag bags upon check-in for certain passengers that automatically are transferred upon U.S. arrival without passenger involvement. Of course, such baggage shall be available, upon landing, for random inspection by CBP through the use of technology or canines.

Problem

One of the greatest challenges CBP and TSA face is identifying international travelers who may pose a threat, distinguishing them from the mass of the traveling public and subjecting them to additional scrutiny in a manner that facilitates the travel of other passengers.

In the Global Entry program, CBP uses a risk-based approach to facilitate the entry of pre-approved U.S. citizens, U.S. nationals, lawful U.S. permanent residents, and citizens of certain other approved countries. Over 100,000 Americans are enrolled in Global Entry as of the end of 2010.[53] This program allows frequent international travelers who pass a background check to use an automated kiosk to clear passport control and to use an expedited line to exit CBP's processing areas. This program is an excellent risk management tool for DHS and a model for TSA.

Moving forward, DHS has an opportunity to utilize Global Entry and other such programs to streamline the aviation screening process for continuing international travelers.

Solution

Expand trusted traveler programs to qualified international passengers. **DHS should expand access to international trusted traveler programs for international passengers entering the U.S., as well as lead efforts to establish a multinational network of streamlined entry procedures for low-risk travelers.**

> "DHS and CBP deserve great credit for developing and enrolling hundreds of thousands of low-risk travelers in Global Entry to shift screening resources to less-known, riskier travelers. To truly capture the benefit of Global Entry, however, the broader U.S. government and industry sectors need to assist CBP in negotiating more bilateral and multilateral agreements to encourage international travelers to enroll in trusted traveler programs."
> —Mr. Sam Gilliland

CBP should accelerate negotiations with countries to develop bilateral trusted traveler programs and identify specific populations of other in-bound travelers to enroll in Global Entry. CBP works with a wide range of countries to develop bilateral trusted traveler programs and successfully developed partnerships with Canada, Mexico, and the Netherlands.[54] However, negotiations with the United Kingdom, Germany, Singapore, and other countries are either bogged down over privacy issues or are at a fledging state. In addition, CBP should consider offering application eligibility to specific classes of individuals whose entry into the U.S. is a national priority either because of their work for international organizations or their potential contributions to our economy.

Once a TSA Trusted Traveler program is created, DHS should cross-enroll travelers between TSA's program and international trusted traveler programs such as Global Entry.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01281 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.913

To the extent that private sector companies continue to offer domestic Registered Traveler programs, CBP should also work on cross-enrollment opportunities with those vendors.

Problem

Despite working in the same airport environment, CBP and TSA operate independently, with little or no coordination on scheduling, training or legal authorities.

TSA and CBP operate under completely different legal regimes, maintain separate workforces, and are generally independent agencies. Cooperation between the agencies tends to depend on the particular relationships at each international airport.

However, to the traveler, both agencies are part of the Department of Homeland Security and of the U.S. government more broadly, and many travelers express frustration about the lack of coordination between CBP and TSA to resolve questions about connecting baggage and flights. Ideas such as cross-training and unifying schedules to take advantage of the variety in flight schedules fall victim to bureaucratic and legal obstacles.

Solution

Eliminate duplication between TSA and Customs and Border Protection. DHS should streamline its operations at U.S. international airports to reduce unnecessary duplication and leverage CBP and TSA resources, authorities, and capabilities.

> "If one keeps going up the chain of command, CBP and TSA employees all have the same boss and it's time for both agencies to start acting like it. We can make noticeable improvements in customer service and airport efficiency simply by coordinating the resources and better utilizing personal that have worked under the same roof for almost a decade." —Mr. Bob Crandall

DHS should assess how to better coordinate TSA and CBP processes at international airports and review whether creating common uniforms, branding and coordinated schedules would allow for more efficient staffing for in-bound and out-bound responsibilities. Any recommendations coming from this review needs Congressional buy-in and a review of any possible synergies between the two large workforces.

As noted above, in the State of the Union, President Obama committed to develop possible government reorganization proposals. Looking for synergies between the sister agencies of CBP and TSA operating at our airports is an appropriate candidate for this review.

In addition, at the local level, for airports offering international service, DHS should negotiate with airports and airlines on issues such as staffing, physical footprint, and equipment deployment from a departmental perspective rather than via different agencies.

Problem

International standards for aviation security are inconsistent and, all too often, unenforced.

The international nature of aviation requires cooperation from a wide range of governments and aviation stakeholders to contribute to U.S. security and efficiency. The U.S. needs to continue to push for international cooperation in the development of international aviation security, including both bilateral and multilateral approaches as needed.

While international aviation security cooperation is improving, as demonstrated by Secretary Napolitano's outreach over the past year to leaders in various regions, more must be done to implement security measures that will enhance the safety of the traveling public and interdict terrorist travel. Some of these efforts are not easily addressed by International Civil Aviation Organization (ICAO) and might be better addressed through continued engagement by DHS and TSA with select nations. While DHS is pursuing enhancements to international standards through ICAO and other multinational organizations, it is not clear that the U.S. government is utilizing its full diplomatic powers on a bilateral basis to implement the standards by exerting pressure, providing training and resources, or whatever is needed in particular cases to influence countries that should be providing assistance as well as those countries that represent the weak link in the international travel system.

In early October 2010, at ICAO's 37th Assembly in Montreal, Canada, the organization endorsed the ICAO Comprehensive Aviation Security Strategy (ICASS) that, among other things, set a new standard for global collaboration to deal with terrorist threats against commercial airlines.[55] This standard built upon five regional security agreements initiated by DHS. Among the areas addressed in the ICASS are:

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01282 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.914

- Capacity-building efforts to help nation states correct vulnerabilities and deficiencies in their security programs;
- Security awareness, training, and advisory services to boost ICAO efforts in aviation security matters; and
- Endorsement of the Implementation Support and Development Security Program (ISD-Security) that promotes regional and cooperative aviation security programs as well as coordination and cooperation with international agencies and donor nations that could assist with building aviation security capabilities globally.

One particular looming problem is the disconnect between the U.S and the European Union on carrying liquids on board commercial airliners. The EU recently announced plans to screen liquids beginning in April of 2011, but the U.S. has not changed its current "3-1-1" regulations. It is possible that EU airports may have to set up separate checkpoints for flights bound to the U.S. and passengers will likely be confused by the disparate treatment.[56]

Solution

Push for international cooperation with U.S. security standards. The federal government must continue to push for international cooperation in the development of international aviation security, including both bilateral and multilateral approaches, as well as with organizations like ICAO, to strengthen aviation security efforts while promoting travel and protecting travelers' rights.

> "Companies that sell security technology do so in a global marketplace. In order to generate cost savings and technological advances for all buyers in that marketplace, the federal government should aggressively embrace global standards and having leading nations pledge to collaborate on this quest." —Mr. Ajay Mehra

Within the next year, DHS should work closely with ICAO to institute strong aviation security standards that complement existing standards and increase adoption of those standards, especially through technical assistance to developing countries in skill-based areas such as workforce development and training.

Building on its current efforts, DHS should work with other Administration officials to prioritize engagement in bilateral or discreet multilateral (i.e. a small subset of G8 nations) discussions to set standards and mutual recognition processes and procedures that cannot be currently readily addressed by ICAO. Among the areas that should be addressed are the following:

- Passenger screening for explosive detection;
- Baggage screening for explosive detection; and
- Cargo on commercial passenger aircraft

The Administration should also support the development of effective international information sharing mechanisms that allow DHS to more readily interdict dangerous passengers. Information sharing mechanisms should address the sharing of information relating to terrorist and criminal watch lists, and passenger information.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01283 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

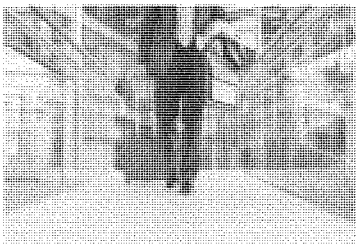
67123.915

GOAL No. 3

Restructure Our National Approach to Aviation Security by Developing and Utilizing Real Risk Management Methods and Tools

"The self-appointed guardians of privacy and tribunes of all sensitivities operate in a state of unreality, complaining both about the sophisticated, data-driven techniques that can help prevent terrorism and the primitive, abuse-inviting, hands-on techniques that have been used instead, the over-application of which is necessitated in no small part by the forbidding of alternatives.... [I]t is the policy, not [TSA], that is the problem."

NATIONAL REVIEW[57]



Today, legislative and executive branch officials talk a lot about "risk management", and how this is a critical part of the nation's security strategy and philosophy. In other areas of homeland security, Congress and DHS made considerable progress in allocating resources according to risk, including grant distribution and CBP programs such as Global Entry. Unfortunately, in the domestic aviation arena, our political leaders do little to actually test and deploy solutions that are important, but not game-changing, improvements over current ones. This situation is due largely to the lack of understandable, quantifiable tools that allow government officials to make data-driven decisions on different security alternatives.

Unfortunately, the homeland security community can do little more than talk about risk management because the tools to help make risk-based decisions do not exist today. As a result, government leaders cannot formally asses the trade-offs between alternatives—making it difficult to deploy policies that are less than a perceived 100 percent, one-size-fits-all solution.

Problem

TSA and Executive Branch officials are not given the tools needed to effectively assess risks and make sound security decisions.

"Two words: Acceptable risk. Instead of acceptable risk we have adopted a zero risk policy, which only means that we've set ourselves up to fail?" —C.B., *YourTravelVoice.org, 11/17/2010*

While policymakers pay considerable "lip-service" to managing risk, executive branch officials are not given the tools needed to effectively assess risks and make sound security decisions. Instead today's security system piles one program on top of another without looking for duplication or whether each additional layer effectively builds on prior, existing programs.

TSA is often a reactive organization, constantly building out new programs, processes or technologies in response to an

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01284 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.916

actual or thwarted attack. Hardened cockpit doors were put in airplanes in response to the 9/11 attacks; the 3-1-1 program to limit the amount of liquids a passenger can bring on an airplane was the result of an aborted attack on U.S. bound aircraft in August of 2006; and deployment of Advanced Imaging Technologies at checkpoints was deployed in response to the December 25 attempted airline bombing. Additionally, TSA has been forced to implement reactionary Congressional mandates that tend to impose new requirements (like 100 percent screening of air cargo) on the organization.

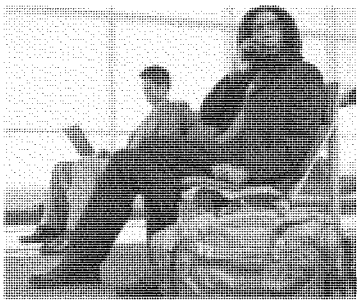
The sum of this constant adding of tools and technologies, whether by TSA or by Congress, has been consistently referred to as "layered" security, with the idea being one layer building upon another and makes the aviation security system better.

Unfortunately, our aviation system is not a symphony of tools and technologies playing in harmony and efficiently moving passengers through security, but instead a cacophony of disjointed parts that are not built to systematically manage risk in the best way possible. Because of the lack of analytical tools and risk management metrics, as well as general public acceptance that there is risk inherent in air travel (as there is with every other mode of travel), new technologies, solutions or tools are often deployed by TSA only in reaction to public events and political pressure.

Risk management methodologies, tools and techniques can help TSA make more data driven decisions. Furthermore, a greater public understanding of these methodologies, tools and techniques can help Congress resist temptation to mandate actions which may not fit within TSA's overall risk management strategy. One only needs to look at the December 25, 2009 underwear bomber—and the resulting rush to expand deployment of Advanced Imaging Technology equipment—to see the latest implementation of this rush to deploy technology that is not necessarily ready for widespread deployment.

As the GAO found in a 2009 study:

> TSA stated that in general, intelligence, vulnerability assessments, scientific analysis, proxies for consequence, security incidents, 9/11 Commission Act requirements, and other relevant information informed TSA's determination of which threats were and were not to be high-risk focus areas. However, these activities do not meet the [National Infrastructure Protection Plan] criteria for credible and comparable risk assessments that integrate assessments of threat, vulnerability, and consequence in a way that is documented, transparent, reproducible, and accurate. Credible risk assessments are particularly important to ensure that resources are directed to programs that address threat scenarios of relatively higher rather than relatively lower risks. Were credible and comparable risk assessments, such as those described in the NIPP, conducted for terrorism threat scenarios, the agency would be able to compare the relative risks of different types of terrorist acts.[58]



This failure is due to a variety of factors. First, TSA does not have the risk management tools or technologies needed to really revolutionize checkpoint security and help policymakers understand the trade-offs between risk, expense and travel efficiency. As a result, decisions are generally made with one risk—the possibility of political outcry—outweighing most others. TSA decision-makers simply do not have the tools to make a decision that might be politically unpopular but effective in managing risk. There are also no tools to help make data driven decisions that can help fend off political attacks.

The DHS effort to develop a long-term planning capability via the Quadrennial Homeland Security Review is generally viewed as a list of priorities rather than a device to force difficult decisions between competing priorities. As Senator Susan Collins, the Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs, commented:

> "As has been stated many times, if you try to protect everything, you end up protecting nothing. So, it is incumbent upon the Department—particularly when budgets are tight—to set detailed priorities to improve the preparedness and security of our nation. The Department's Quadrennial Homeland Security Review (QHSR) was a good first attempt to outline strategic homeland security missions and goals. Yet, the Department acknowledged that the QHSR was

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01285 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.917

incomplete, so it conducted a follow-on review. This assessment, known as the "Bottom-Up Review" (BUR) was intended to set priorities for security initiatives and reorganization at the Department.

While I appreciate the Department's effort to undertake such a comprehensive analysis, the results are disappointing. Indeed, the two reviews simply don't compare to the level of planning and analysis that goes into the Quadrennial Defense Review and supporting documents.... By comparison, the QHSR and BUR amount essentially to high-level strategy documents that provide little in the way of concrete goals or the actions needed to achieve them."[59]

TSA does little to actively cultivate relationships with stakeholders it does not regulate directly. The organization has elaborate and meaningful relationships with its regulated parties—commercial aviation companies, airports, cargo airlines, pipeline owners, mass transit, etc.—as it should. However, TSA consistently fails to engage the millions of travelers—business or leisure—who rely on predictable, safe, efficient transportation. As a result of this myopic approach, TSA has developed little political support nor an effective advocacy community that can help create a political climate conducive to policies that might be unpopular but effective from a risk perspective.

Solution

Implement well-defined risk management processes. The Administration should convene an external panel of experts with appropriate security clearances to review TSA aviation security programs, assessing the risk each is designed to mitigate and develop metrics for measuring progress to lessen that risk.

"Expertise in risk mitigation exists in both the public and private sectors. We should accept nothing less than bringing together the best and the brightest in an effort to develop the tools and technologies needed to manage risk, set priorities and measure progress." —The Honorable Tom Ridge

This panel of experts should formally agree upon the highest aviation security risks that be addressed and develop metrics to measure success in mitigating these risks. Once the security risks being addressed by each program are understood and metrics agreed to by the panel, the each aviation security program should be graded. For programs that are deemed successful, success factors should be identified, and future program development (or termination) should be outlined. For programs that are deemed unsuccessful by the metrics agreed to, the external panel of experts should outline options for improving these programs and provide recommendations.

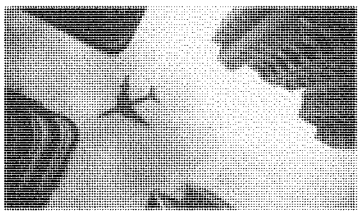
For instance, the Federal Air Marshals Program (FAMS), continues to account for around 12 percent of TSA's budget. The FAMS program was originally expanded after 9/11 to provide a last line of defense when the other layers of aviation security were being improved and at a time when cockpit doors were not yet hardened against intrusion. The appropriate level of the FAMS program, both for international and domestic flights, is an example of a review that should be evaluated in a risk management context.

Furthermore, Congress should authorize and appropriate sufficient funds for the development of analytical tools that will allow government agencies to better measure the risks that individuals might pose to the commercial aviation system. Such an effort, if constructed properly, could be a good stepping stone for assessment of traveler risk in a range of modes of transportation, and for a range of government programs. Whether housed at TSA or elsewhere, this capability should be utilized not only by TSA but by CBP and any other DHS component that is assessing traveler risk.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01286 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.918

Blue Ribbon Panel for Aviation Security



Panel Co-Chairs

The Honorable Tom Ridge, former Secretary of the U.S. Department of Homeland Security, currently CEO of Ridge Global

The Honorable Jim Turner, former Ranking Democratic Member of the House Homeland Security Committee, currently Partner at Arnold & Porter

Sam Gilliland, Chairman and CEO of Sabre Holdings

Members

Bob Crandall, former CEO of American Airlines

Jessica Herrera-Flanigan, former Staff Director of the House Homeland Security Committee

The Honorable Kathryn "Kitty" Higgins, former Board Member of the National Transportation Safety Board

Ajay Mehra, Executive Vice President at OSI Systems and President of Rapiscan Systems

Rick "Ozzie" Nelson, Director of Homeland Security and Counterterrorism Program at the Center for Strategic & International Studies

Thomas Ripp, President of L-3 Security and Detection Systems

David Bronczek, President and CEO of FedEx Express

Fred Dust, Partner and Practice Lead at IDEO

Kevin Hassett, Senior Fellow and Director of Economic Policy Studies at American Enterprise Institute

Frank Miller, Aviation Director, San Antonio Airport System

Rick Patrick, Executive Vice President, Digital Sandbox

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01287 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.919

APPENDIX

The History of Aviation Security and TSA's Current Security Framework

History of Aviation Security Pre-September 11, 2001

Prior to November 2001, the Federal Aviation Administration (FAA) controlled aviation security at U.S. airports. The FAA promulgated rules and regulations governing the aviation security but largely delegated the execution of these responsibilities to individual airlines. Most airlines, in turn, contracted with private security vendors to carry out the physical screening of passengers and carry-on baggage.

During the 1960s and early 1970s, several deadly hijackings and terrorist bombings had prompted changes to the U.S. aviation security regime. In 1970, President Richard Nixon created an anti-hijacking program, which included the creation of Federal Air Marshals service. Then, in 1973, the FAA issued an emergency rule making requiring airlines to conduct inspection and screening of all carry-on baggage and passengers aboard commercial airlines. In 1974, Congress enacted legislation codifying the FAA's 1973 emergency rulemaking and required the continued screening of all carry-on baggage and passengers aboard commercial airlines.

Over the next 27 years until the events of September 11, 2001, aviation security in the United States remained largely unchanged despite continued threats and successful attacks against U.S. commercial airlines.

Creation of TSA and the Federalization Aviation Security

The events of September 11, 2001, brought a renewed focus on securing American's transportation system from the threat of terrorist attacks.[60] In response to the risks posed to the nation's transportation system by domestic and international terrorism, Congress passed the Aviation and Transportation Security Act (ATSA), which was signed into law on November 19, 2001.[61] ATSA created the Transportation Security Administration (TSA), within the Department of Transportation (DOT), as the principal agency responsible for security of all modes of transportation. In 2002, Congress passed the Homeland Security Act of 2002, which transferred TSA into the newly created Department of Homeland Security (DHS), and committed further resources and regulatory strength to protecting American's transportation systems.[62]

Under its enacting charter, TSA is responsible for the complex task of ensuring the freedom of movement of goods and people by providing security over all modes of transportation, including rail, mass transit, trucking, bus and aviation security. However, since 2001, the agency has focused the majority of its resources and personnel on aviation security.

In creating TSA, ATSA made several significant changes to the pre-9/11 aviation security regime. First, TSA was charged with carrying out both the regulatory and operational responsibilities of aviation security, and ATSA required all transportation security workers to be federal employees.[63] Second, ATSA mandated that 100 percent of checked luggage on all commercial flights be screened for explosives and other dangerous materials, and issued strict timelines for implementation. Third, TSA required the screening of all individuals, vehicles and property entering into secured areas of an airport. Fourth, TSA created a number of programs designed to provide additional layers of security even if a terrorist was able to board an aircraft including: 1) a massive expansion of the Federal Air Marshal Service (FAMS),[64] the arming of trained pilots under the Federal Flight Deck Officer (FFDO) program, and perhaps most importantly, the requirement that all cockpit doors be hardened to reduce the chance of hijacking.

Current Overview of TSA Workload, Staffing and Funding Levels

Over the past decade, TSA has evolved to implement several new programs and policies in the area of aviation security. TSA's current responsibilities include:

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01288 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.920

The History of Aviation Security and TSA's Current Security Framework

- Providing security services at airport access points, passenger screening checkpoints, and other sensitive areas in and around U.S. airports;
- In flight detection and deterrence of criminal and terrorist activities;
- Pre-screening of airline passengers against terrorists watch lists through the Secure Flight Program;
- Airline passenger screening and identity verification;
- Screening of carry-on and checked baggage, and air cargo for explosives and other dangerous materials;
- Credentialing and screening of airport employees;
- Training and deployment of Transportation Security Officers (TSOs), Behavioral Detection Officers (BDOs), Transportation Security Inspectors (TSIs), and National Explosives Canine Detection Teams;
- Administering security training and partnerships programs, such as Crew Member Self Defense and the FFDO; and
- Oversight, inspection and investigation of compliance with TSA regulations and security practices.

TSA is also responsible for several aspects related to international aviation security, in partnership with other U.S. federal agencies, international aviation stakeholders, and foreign governments. Among TSA's responsibilities on the international front are:

- Inspecting air carrier operations to the U.S.;
- Assessing security of airports overseas;
- Ensuring foreign airport compliance with TSA security requirements;
- Advising foreign governments on transportation security;
- Training overseas security personnel;
- Ensuring implementation of international security standards;
- Reviewing threat mitigation strategies for foreign airports;
- Working with non-U.S. air carriers to achieve regulatory compliance; and
- Assisting foreign governments to achieve sustainable security capacity.

In addition, TSA works closely with the Science & Technology Directorate (S&T) at DHS, which is responsible for the research and technology development programs related to aviation security. S&T has especially been involved in development and deployment of airport passenger screening and explosive detection technologies.

In the area of aviation security alone, the workload of TSA is monumental. TSA currently conducts passenger and baggage screening at about 450 U.S. airports, which house over 750 screening checkpoints and 2,200 security lanes. In 2009 alone, TSA screened an average of 2 million aviation passengers per day and over 625 million domestic passengers over the entire year. In addition, TSA now screens, on average, roughly 1.5 million bags per day.

At present, TSA employs over 62,000 federal workers to execute its mission and programs, making it one of the largest federal agencies in the country. The majority of TSA employees are airport security screeners, known as Transportation Security Officers ("TSO's") which would total almost 50,000 workers (about 80% full-time employees). TSA also has a sizable administrative staff of approximately 3,650 employees.

In its FY 2012 budget request, the DHS requested an increase to the funding for TSA to $8.1 billion including mandatory fees, nearly all of which is devoted directly to aviation security or to support the overall TSA mission. A significant amount of the increased funding request was designed to address passenger and international security, including the addition of 5,355 full and part-time TSOs, enhancements of passenger and baggage screening technology, and deployment of additional explosive detection canine teams.

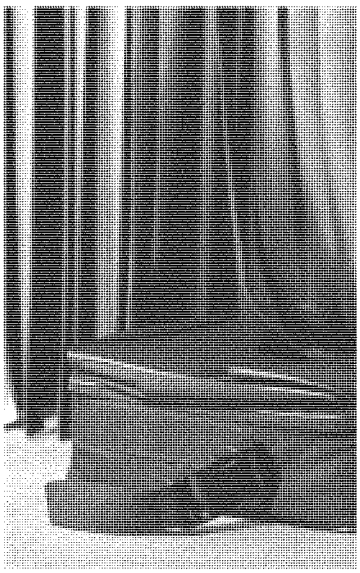
Airline Passenger and Baggage Screening: Past and Present

In implementing ATSA, TSA constructed a layered approach to aviation security including new procedures and technologies generally not in use before 9/11. TSA has described the "layering" of security as follows:

> We use layers of security to ensure the security of the traveling public and the Nation's transportation system. Because of their visibility to the public, we are most associated with the airport checkpoints that our Transportation Security Officers operate. These checkpoints, however, constitute only one security layer of the many in place to protect aviation… Each one of these layers alone is capable of stopping a terrorist attack. In combination their security value is multiplied, creating a much stronger, formidable system. A terrorist who has to overcome multiple security layers in order to carry out an attack is more likely to be pre-empted, deterred, or to fail during the attempt.[65]

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01289 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.921



While all carry-on baggage and commercial aviation passengers were required to be screened prior to 9/11, the additional security methods deployed by TSA when it commenced operations in 2002 included:

- each ticketed passenger to display a valid government ID before entering the security checkpoint and boarding a commercial flight;
- Screening of all checked baggage for explosives, prohibited items and other dangerous materials;
- Restricting certain dangerous items, such as scissors, knives, butane lighters and box cutters, from being carried aboard an airplane's passenger cabin; and
- Allowing only ticketed passengers, airport and airline employees, and certain approved law enforcement officials beyond the passenger screening checkpoints.

All of the procedures mentioned above remain in place today, although some of the screening technology has been updated and improved. However, in response to several attempted terrorist attacks over the past 10 years, Congressional mandates, recommendations of the 9/11 Commission and the Government Accountability Office (GAO), and self imposed directives and regulation, TSA has continually added additional layers of security to its initial procedures. The following is a list of procedures, technologies and requirements that TSA currently utilizes, along with the reason for their deployment:

- **Removal of shoes when passing through security checkpoints**—implemented in December 2001 after an Al Qaeda operative attempted to blow up American Airlines Flight 63 using explosives hidden in the soles of his shoes;
- **Ban of liquids, gels, and certain food items in excess of 3 ounces from being carried onto a commercial flight**—implemented in August 2006 after a terrorist plot to smuggle liquid explosives onto aircraft was uncovered in Great Britain;
- **Removal of laptops, video cameras and other large electronics in carry-on bags for separate x-ray screening**—implemented in August 2007 in response to known terrorist threats;
- **Use of Advance Imaging Technology (AIT) machines for primary and secondary passenger screening**—accelerated deployment for widespread use at major airports beginning early 2010 in direct response to the attempted bombing of Northwest Airlines Flight 253;
- **Use of enhanced passenger pat-downs for secondary and random screening of passengers**—implemented in October 2010, also in response to the attempted bombing of Northwest Airlines Flight 253;
- **Name matching of airline passengers against government watch lists through the Secure Flight Program**—implementation from January 2009 until full implementation in November 2010.

The creation of DHS in 2003 also resulted in changes for international border processing. The U.S. Customs Service, transferred from the Department of Treasury, and a piece of the dismantled Immigration & Naturalization Service were

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01290 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.922

merged to create U.S. Customs & Border Protection (CBP). CBP is primarily responsible for securing the borders at and between the ports of entry as well as facilitating legitimate travel into the U.S.

Both TSA and CBP have national security responsibilities in the international travel continuum that involve significant interaction with the traveling public and often with the very same travelers on a single trip. However, they tend to operate as completely distinct entities despite their complementary capabilities and authorities related to both security and facilitation and the fact that DHS was created to find synergies across its large operational agencies to meet the department's vast responsibilities.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01291 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.923

Endnotes

[1] Consensus Research Group, Inc., "A Study of Air Traveler Perceptions of Aviation Security Screening Procedures", December 15, 2010, www.ustravel.org/news/press-releases/american-traveling-public-says-there-has-be-better-way-conduct-air-travel-secu

[2] "Remarks by the President in State of Union Address", January 25, 2011, www.whitehouse.gov/state-of-the-union-2011

[3] 526 U.S. 489 (1999)

[4] *Kent v. Dulles*, 357 U.S. 116 (1958)

[5] U.S. Department of Homeland Security, "Secretary Napolitano Outlines Five Recommendations To Enhance Aviation Security", January 7, 2010, www.dhs.gov/ynews/releases/pr_1262907427865.shtm

[6] Federal Aviation Administration, "The Economic Impact of Civil Aviation on the U.S. Economy", December 2009, www.faa.gov/air_traffic/publications/media/FAA_Economic_Impact_Rpt_2009.pdf

[7] U.S. Department of Transportation, Bureau of Transportation Statistics, "National Household Travel Survey", May 2006, www.bts.gov/programs/national_household_travel_survey/

[8] The sampling of the 2008 Peter D. Hart Research Associates and The Winston Group survey is representative of the entire U.S. air traveling public, with a statistical margin of sampling error of ±3.2 percentage points. www.ustravel.org/news/press-releases/air-travelers-avoided-41-million-trips-past-year-us-economy-takes-265-billion-hi

[9] Consensus Research Group, Inc., "A Study of Air Traveler Perceptions of Aviation Security Screening Procedures", December 15, 2010, www.ustravel.org/news/press-releases/american-traveling-public-says-there-has-be-better-way-conduct-air-travel-secu

[10] U.S. Government Accountability Office, "Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation", March 27, 2009, www.gao.gov/new.items/d09492.pdf.

[11] U.S. Department of Homeland Security, "Budget & Finance", www.dhs.gov/xabout/budget/

[12] Bureau of Transportation Statistics, "Passengers: All Carriers, All Airports", www.transtats.bts.gov/Data_Elements.aspx?Data=1

[13] Federal Aviation Administration, "FAA Aerospace Forecasts FY 2011-2031", Washington, D.C., February 14, 2011, www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2011-2031/

[14] Alan Levin, "FAA forecasts 80% increase in fliers by 2031", February 15, 2011, http://travel.usatoday.com/flights/story/2011/02/FAA-forecasts-80-increase-in-fliers-by-2031/43779428/1

[15] Kip Hawley, *Los Angeles Times*, "Plugging the airport security gaps", January 29, 2011, www.latimes.com/news/opinion/commentary/la-oe-hawley-tsa-20110129,0,5091218.story

[16] Remarks of Norman Y. Mineta, Secretary of Transportation, Travel and Tourism Industry Unity Dinner, March 6, 2002, Washington D.C.

[17] U.S. Government Accountability Office, "Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed", February 28, 2007, www.gao.gov/products/GAO-07-299

[18] The issues related to visa issuance, international watchlists, and inter-agency cooperation, all found wanting in the after-action reports on the Abdulmutallab case, are beyond the scope of this report, although crucial to international travel security. "White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack", www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack

[19] The TSA experience may be particularly daunting to foreign visitors who travel within the U.S. and depart from U.S. airports. As a federal advisory committee reported to DHS and the Department of State in 2008: "[S]tatistics, public opinion studies, and anecdotal evidence show that the policies put in place to make our borders more secure are perceived as making travel to the U.S. more difficult and unpleasant for many foreign visitors than before 9/11 and in comparison to other countries". Report of the Secure Borders and Open Doors Advisory Committee (SBODAC), www.dhs.gov/xlibrary/assets/hsac_SBODACreport508-compliant_version2.pdf, p. 5.

[20] Testimony of Department of Homeland Security Secretary Janet Napolitano, U.S. Senate Committee on Commerce, Science and Transportation, January 20, 2010, http://commerce.senate.gov/public/?a=Files.Serve&File_id=e5b29bd1-2ded-491e-83dc-f62852eb46b2

[21] U.S. Department of Homeland Security, "Secretary Napolitano Announces New Measures to Strengthen Aviation Security", April, 2, 2010, http://www.dhs.gov/ynews/releases/pr_1270217971441.shtm

[22] Robert Poole, "Airport Security: Time for a New Model", January 2006, Washington, D.C., http://reason.org/news/show/127389.html

[23] Jay Stanley, "Airline Passenger Profiling: Back From the Grave?", February 8, 2011, www.aclu.org/blog/technology-and-liberty/airline-passenger-profiling-back-grave

[24] Charles Krauthammer, "Don't touch my junk," November 19, 2010, www.washingtonpost.com/wp-dyn/content/article/2010/11/18/AR2010111804494.html

[25] Harriet Baskas, "TSA embraces new medical notification cards", December 14, 2010, www.msnbc.msn.com/id/40647207/ns/travel-news/; Cordova Times, "Begich addresses TSA methods of screening passengers", http://thecordovatimes.com/article/1109begich_addresses_tsa_methods_of_screening

[26] CBS News, "Poll: Most Support New TSA Measures", December 3, 2010, www.cbsnews.com/8301-503544_162-20024625-503544.html

[27] Public Law 107-71, Section 109: "The Under Secretary of Transportation for Security may … (3) Establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.

[28] U.S. Transportation Security Administration, "The program is a market-driven venture offered by the private sector in partnership with airports and airlines." www.tsa.gov/approach/rt/index.shtm

[29] Thomas Frank, "TSA's Registered Traveler program grounded", June 23, 2009, www.usatoday.com/travel/flights/2009-06-22-frequent_N.htm

[30] CLEAR is operating at Denver and Orlando, while the IQueue program operates in Indianapolis. www.clearme.com; www.flyiqueue.com.

[31] John Pistole, "Providing Security and Respecting Privacy: TSA's Efforts to Protect the American People", *American Bar Association*, January 13, 2011, www.c-spanvideo.org/program/SecurityandPr

[32] 49 C.F.R. 1542.209(d).

[33] See, e.g., United's Premiere Line Access, store.united.com/traveloptions/control/category?category_id=UM_PMRTRVL&navSource=Travel+Options+Main+Menu&linkTitle=UM_PMRTRVL#airAnchor; Delta Sky Priority, delta.com/traveling_checkin/airport_information/frequent_traveler_security/index.jsp

[34] Jayne Clark, "A day in the life of an airport screener", September 7, 2006, www.usatoday.com/travel/flights/2006-09-07-tsa-screener_x.htm; John Krieser, "The TSA's Warehouse Of The Weird", February 9, 2006, www.cbsnews.com/stories/2006/02/09/eveningnews/main1302676.shtml

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01292 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.924

Endnotes

[35] Natalie Avon, "Airline baggage fees top $2.5 billion", December 13, 2010, http://articles.cnn.com/2010-12-13/travel/baggage.cancellation.fees_1_baggage-fees-ancillary-fees-change-fees?_s=PM:TRAVEL

[36] Associated Press, "More carry-ons costing TSA millions each year", March 4, 2011, http://voices.washingtonpost.com/federal-eye/2011/03/more_carry-ons_costing_tsa_mil.html

[37] "Remarks by the President in State of Union Address", January 25, 2010, www.whitehouse.gov/state-of-the-union-2011

[38] U.S. Government Accountability Office, Aviation Security: TSA's Cost and Performance: Study of Private-Sector Airport Screening, January 9, 2009, www.gao.gov/new.items/d09927r.pdf

[39] U.S. Transportation Security Administration, "TSA Statement on Contractor Screening Program", January 28, 2011, www.tsa.gov/press/happenings/2011/012811_contractor_screening_program.shtm

[40] U.S. Transportation Security Administration, "TSA Administrator: 'We Will Not Negotiate on Security'", February 4, 2011, www.tsa.gov/press/releases/2011/0204.shtm

[41] House Committee on Transportation and Infrastructure Chairman John Mica (R-FL), "TSA Keys Handed to Unions", February 4, 2011, http://transportation.house.gov/news/PRArticle.aspx?NewsID=1063

[42] Administrator Pistole indicated in recent congressional testimony that DHS may be reinstating a department-wide ASAC. U.S. House of Representatives Committee on Homeland Security, Subcommittee on Transportation Security, "Terrorism and Transportation Security", February 10, 2011, http://homeland.house.gov/hearing/subcommittee-hearing-%E2%80%9Cterrorism-and-transportation-security%E2%80%9D-0.

[43] The White House, "Transparency and Open Government, Memorandum for the Heads of Executive Departments and Agencies", www.federalregister.gov/articles/2009/01/26/E9-1777/transparency-and-open-government

[44] The 9/11 Commission recommended that Congressional oversight of DHS be streamlined, and Commissioners continue to advocate this recommendation. National Commission on Terrorist Attacks Upon the United States (9/11 Commission Report), p 421, http://govinfo.library.unt.edu/911/report/index.htm; Testimony of Lee Hamilton and Tom Kean, House Committee on Homeland Security, "Viewpoints on Homeland Security: A Discussion with the 9/11 Commissioners", May 21, 2010, http://chsdemocrats.house.gov/SiteDocuments/20100519102120-36576.pdf

[45] Patrick Marshall, "A surfeit of RFPs?", October 7, 2007, http://gcn.com/articles/2007/10/07/a-surfeit-of-rfps.aspx?sc_lang=en

[46] U.S. Transportation Security Administration, "News & Happenings: Checkpoint Friendly" Laptop Bag Procedures", August 15, 2008, www.tsa.gov/press/happenings/simplifying_laptop_bag_procedures.shtm

[47] Agam Shah, "Laptops Lost Like Hot Cakes at US Airports", June 30, 2008, www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airports.html.

[48] U.S. Transportation Security Administration, "The TSA Blog: Traveling with E-readers, Netbooks, and Other Small Gadgets (Including the iPad)", April 6, 2010, www.tsa.gov/blog/2010/04/traveling-with-e-readers-netbooks-and.html

[49] Public Law 111–83, Department of Homeland Security Appropriations Act, 2010, Section 537.

[50] Public Law 109-13, 'Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005', Title II; National Conference of State Legislators, "Count down to REAL ID", www.ncsl.org/default.aspx?tabid=13577; Janice Kephart, "REAL ID Implementation: Less Expensive, Doable, and Helpful in Reducing Fraud", January 2011, http://cis.org/real-id

[51] See SBODAC, p. 37. ("The Departments also should develop a national program to encourage all high school graduates to obtain a passport at the same time they receive their diploma and/or register for the Selective Service.")

[52] See SBODAC at p. 34 ("Wherever possible, the redundant requirement to re-screen checked bags from international connecting flights should be removed.")

[53] U.S. Customs and Border Protection, "CBP's Global Entry Pilot Program Reaches 100,000 Members" December 27, 2010, www.cbp.gov/xp/cgov/newsroom/news_releases/national/12272010_2.xml.

[54] U.S. Customs and Border Protection, "NEXUS and SENTRI Members May Utilize the Global Entry Kiosks", January 3, 2011, www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/ge_kiosks.xml

[55] www.icao.int/icao/en/assembl/a37/wp/wp018_en.pdf

[56] Benet Wilson, "Airlines, Airports Fight New EU Regulations On Liquids Ban", February 24, 2011, www.aviationweek.com/aw/generic/story_generic.jsp?channel=aviationdaily&id=news/avd/2011/02/25/11.xml&headline=Airlines,%20Airports%20Fight%20New%20EU%20Regulations%20On%20Liquids%20Ban

[57] The Editors, "TSA Troubles", November 24, 2010, www.nationalreview.com/articles/253864/tsa-troubles-editors

[58] U.S. Government Accountability Office, "Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation", March 27, 2009, www.gao.gov/new.items/d09492.pdf.

[59] U.S. Committee on Homeland Security and Governmental Affairs, "Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review", July 21, 2010, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=66726e74-1f4e-4395-a5c4-8937437ef8bd

[60] National Commission on Terrorist Attacks Upon the United States (9/11 Commission Report), pp. 390-393, http://govinfo.library.unt.edu/911/report/index.htm

[61] Public Law 107-71.

[62] Public Law 107-296.

[63] ATSA granted TSA authority to allow airports to handle security operations with private contractors acting under TSA regulations and oversight. The pilot program was later branded the Security Partnership Program. www.tsa.gov/what_we_do/oprout/index.shtm

[64] U.S. Transportation Security Administration, "Federal Air Marshal Shortage?", www.tsa.gov/approach/mythbusters/fams_shortage.shtm

[65] U.S. Transportation Security Administration, "What We Do," www.tsa.gov/what_we_do/layers/index.shtm

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01293 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.925

Statement

Of

Kenneth J. Dunlap

Global Director, Security & Travel Facilitation

International Air Transport Association (IATA)

"Ten Years After 9/11: The Next Wave in Aviation Security."

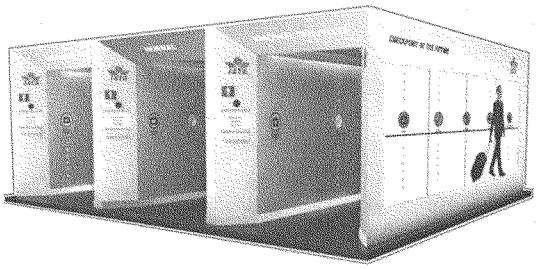
Before the

U.S. Senate

Committee on Homeland Security

And Governmental Affairs

November 2, 2011



VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01294 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.875

Introduction

Chairman Lieberman and Ranking Member Collins, thank you for the opportunity to testify at this hearing. The International Air Transport Association (IATA) appreciates the leadership of the Senate in addressing this critical issue. It is our hope that today's hearing accelerates the much needed dialogue on the future of passenger screening post 9.11 in the United States.

IATA and our 230 US and foreign member airlines have a vision of future passenger screening that is based on a paradigm shift in the principles behind checkpoint operations. We believe next generation checkpoints must focus on looking for "bad people" and not just "bad things."

I would ask that you consider our vision of an effective airport checkpoint:

- Security is enhanced with higher probabilities of detection
- Passengers are treated with dignity
- Babies and children with names similar to adults on the no fly-list pass through screening uneventfully
- Harmless objects such as toenail scissors and nail clippers do not trigger alarms

In this scenario, the airport security checkpoint is no longer a standalone line of defense against terrorism but rather part of an integrated system that uses risk-based analysis as well as advanced screening technology to improve security and the travel experience for the passenger.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01295 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.876

We call this vision "Checkpoint of the Future," and many of the key components are available today.

Why develop a future checkpoint? First, aviation remains a target, as was demonstrated by the December 2009 attempted bombing of a Northwest Airlines flight bound for Detroit. The status quo is not good enough. We must stay ahead of the bad guys.

Second, air travel is forecast to continue growing, and today's checkpoints are already showing their age. IATA expects an additional 90 million passengers will travel within North America between now and 2014 and 659 million new passengers for the entire world. Our long range projections are that by 2050 as many as 16 billion people will fly annually.

But the evidence shows that the throughput of today's checkpoints is decreasing. Our systems just cannot handle the traffic. In some places, we have seen a drop in throughput of as much as 50% in two years.

Some of the decrease was the result of the new security measures put in place after the Christmas Day 2009 attempted bombing. But the rest we believe is the result of a passenger screening system showing its age.

Third, the aviation security system needs to maintain the confidence of the traveling public. Unfortunately, the signs of discontent are growing. Passengers are becoming increasingly vocal about the inconvenience of security measures and the threat to personal privacy. We are seeing protests driven by social media sites. Last year, one group even called for a national opt-out of body scanning on the day before Thanksgiving.

Let me be clear: we have good systems, and the flying public is safe. But we also need a confident public that trusts the authorities. Good systems combined with distrustful passengers make for a toxic combination and a less secure system.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01296 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.877

Lessons Post 9.11

What lessons have we learned in the past decade concerning passenger screening? First, dropping new technology into an old checkpoint will not work. That's akin to placing a new radio in an old car and saying you have a new car. You still have an old car.

Security and technology are often confused. IATA remains concerned that new technology is being viewed as the silver bullet for the future. There is no single silver bullet. For every technology with exciting detection capabilities there are complementary vulnerabilities.

Also, we must not overlook the process through which technology moves from the laboratory to the airport. Fundamentally, the journey takes too long, and it is affected by changing regulatory requirements, often producing a product which doesn't work in the real world. An unfortunate example was the recent failure of the so-called "puffer" explosive detection machines.

Second, object finding has served us well, but does not represent the future. If we have learned anything from the last decade, it is that a passenger with toenail clippers is not automatically a threat to aviation. Alternatively, if you find toenail clippers you have not necessarily found a terrorist.

Third, "one size fits all screening" has outlived its usefulness. Over 2.8 billion passengers are screened per year. We cannot continue at this pace without using risk-based screening measures.

IATA's Way Forward

IATA has been working for the last year and a half on developing a more efficient, effective and relevant checkpoint. Let me spend a few minutes discussing the core principles and explain how we propose turning these into a checkpoint.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01297 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.878

The Checkpoint of the Future described here, relies on two basic concepts. The first is the introduction of risk-based screening, using data from travel documents and airline tickets that is already being used by the US Government and other governments for customs and immigration. Let me emphasize that this does not involve profiling of any kind. We are simply proposing that rather than using this data only at the end of a journey for purposes of border control, we should use it at the beginning of the journey for security purposes.

This process is invisible to the traveler, but it will enable a decision to be made before the traveler arrives at the airport. This fulfills a fundamental principle of the Checkpoint of the Future: passengers should be screened at the airport with devices and processes commensurate with what is known about them.

The second concept is the use of advanced screening technology to enable a seamless journey through the screening lanes without removing items of clothing or unpacking carry-on luggage.

Upon arriving at an airport checkpoint the passenger biometrically identifies himor herself and has a brief encounter with a behavior analyst. The passenger is assigned a lane based on the result of their electronic prescreening or random selection. The passenger proceeds through the lane and is screened while in motion. Passengers who voluntarily opt-in to a known traveler program and agree to provide additional information about themselves would proceed through a known-traveler lane. Those about whom little is known or those randomly selected would go through an enhanced security lane. But let me emphasize that all passengers are screened to a baseline and no one gets a free pass.

In addition to the improved security that will result from the use of risk-based analysis, passengers will also have a better experience. IATA estimates that even using today's technology the increased efficiency translates into as much as a 30% reduction in wait times for passengers.

So where are we and what have we done? IATA has developed blueprints and a roadmap and our Board of Governors has agreed to move forward. We are working

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01298 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.879

with like-minded associations, manufacturers, academics, and airlines to refine this concept. This needs to be a global effort.

To date, ICAO has endorsed the need for a global effort to study a future checkpoint. INTERPOL and 12 states have signed statements of principal that we are going in the right direction.

So where are we on key technology? IATA and our industry technology partners will be working on researching and promoting development of systems to optimize today's checkpoints. We believe that as processes and components are developed they should be made available as toolkits for implementation.

We certainly expect that in seven to ten years all the necessary components for a walk-through screening process will be available. But we can repurpose and reintegrate existing technology into an intermediate checkpoint that is possible in the next 2-3 years.

This reworked checkpoint uses existing hardware and combines several central elements of Checkpoint of the Future including passenger data already being used by governments, behavior analysis, and the creation of new screening lanes.

IATA is committed to making air travel safe, secure, and more enjoyable.
We believe a new passenger checkpoint paradigm is mandatory and needs to be brought to airports at an accelerated pace.

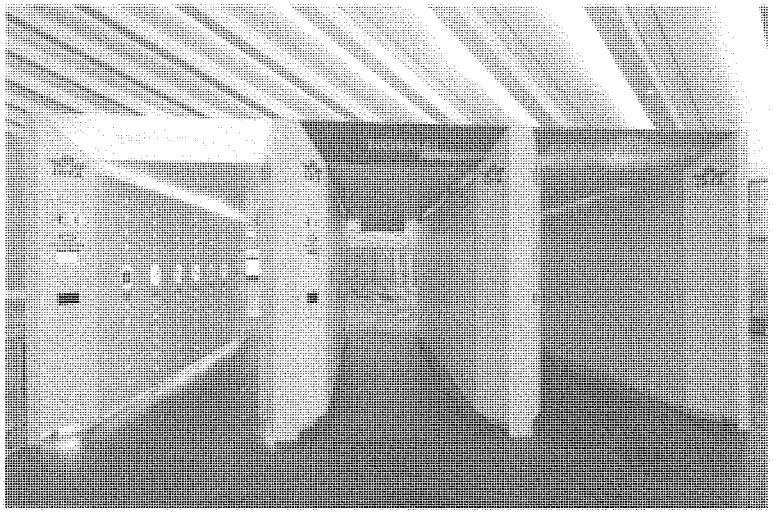
In summary we believe the foundation of the Checkpoint of the Future should be based on lessons learned post 9/11. The next generation of checkpoint should:

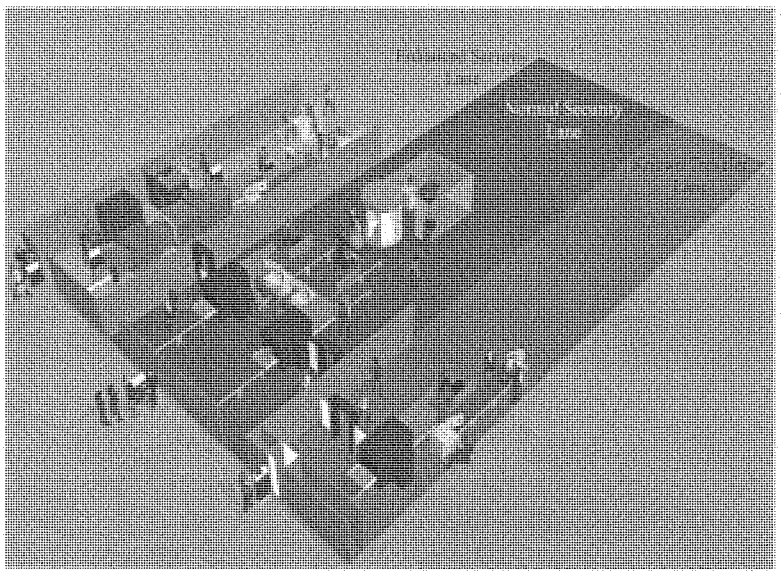
- Use passenger data
- Use behavior detection
- Screen passengers based on risk
- Provide for an uninterrupted journey from curb to aircraft door
- Preserve our investment in existing checkpoints

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01299 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.880

We won't settle for anything less than a revolution in the way passengers are treated at the airport.





Testimony of the International Air Transport Association, Montreal Quebec
Before the Committee on Homeland Security and Government Affairs
November 2, 2011

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01300 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.881

Statement of Charles M. Barclay, A.A.E.
President, American Association of Airport Executives
Before the Senate Committee on Homeland Security and Governmental Affairs
"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

Chairman Lieberman, Ranking Member Collins, and members of the Committee, on behalf of the American Association of Airport Executives and the thousands of men and women the association represents who operate and manage the nation's airports, I want to thank you for the opportunity to participate in this important hearing on the future of aviation security. Public safety and security are a primary focus of AAAE and airport executives, and we remain committed to working with Congress, the Transportation Security Administration and our industry partners to chart a course forward that builds upon the experiences of the past decade to further enhance security, efficiency, and passenger satisfaction.

Airports Partner with TSA on Screening and Perform Inherently Local Security Functions
As you know, airports play a critical role in aviation security, serving as an important partner to TSA in helping the agency meet its core mission of passenger and baggage screening. The significant changes that have taken place in airports over the past decade with the creation of the TSA and its assumption of all screening duties have been aided dramatically by the work of the airport community, and we will serve as a critical local partner to the agency as it continually modifies its operations, including some of the risk-based security initiatives that are under discussion today.

In addition to partnering with TSA to meet its core mission, airports as public entities provide a critical local layer of security, performing a number of inherently local security-related functions at their facilities, including incident response and management, perimeter security, employee vetting and credentialing, access control, infrastructure and operations planning, and a myriad of local law enforcement functions. These important duties have long been local responsibilities that have been performed by local authorities in accordance with federal standards and subject to federal oversight.

Airport operators meet their security-related obligations with a sharp focus on the need to protect public safety, which remains one of their fundamental missions. The professionals who perform these duties at airports are highly trained and have the first responder authorities and responsibilities that we all value immensely. From a security and resource perspective, it is critical that these inherently local functions remain local with federal oversight and backed by federal resources when appropriate.

Looking Forward: Effectively Targeting Limited Resources is Essential
Over the past decade, great strides have been made to enhance security at the nation's airports. Among other things, technology that provides unprecedented screening capabilities has been widely deployed and better integrated into airport terminals, and much more is known about those who work in the sensitive areas at all 450 regulated airports.

The challenge for the next decade and beyond is to more effectively utilize and link technologies and information that separate and scrutinize true threats to the system from those who pose little or no risk. Efforts must also be made in the aviation environment to keep TSA focused on its

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01301 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.882

primary mission of passenger and baggage screening. Expanding the agency's mission – particularly to areas already in capable local hands – threatens to dilute already scarce resources.

The intense pressure on all federal budget resources, continued threats to the aviation system, and growing traffic levels at the nation's airports make the passenger screening protocol that has been in place since 9/11 unsustainable. We simply don't have the resources necessary to continue operating a personnel dependent screening system that treats every traveler the same regardless of the risk they pose to the system.

In our view and in the view of many security experts, one of the key components to improving passenger screening and security is expanding the focus from finding dangerous "things" to finding dangerous "people." After all, the most important weapon that the 19 terrorists had on September 11 wasn't box cutters; it was knowledge – knowledge of our aviation system and existing security protocols, which they used to their advantage.

Recognizing that fact, airport executives and many others have long advocated the adoption of a trusted/known traveler program to better identify and scrutinize potential threats. As you know, the trusted/known traveler concept allows for intense focus on individuals who voluntarily provide information prior to their arrival at the airport, freeing resources at screening checkpoints to focus on those for whom little is known. The result is enhanced security and improved efficiency at screening checkpoints.

The merits of a trusted/known passenger concept are proven and well documented, and the approach has been endorsed by a number of key groups, including the 9/11 Commission. Trusted traveler programs also received prominent attention in the recommendations of then-Secretary Mineta's high-level airport security Rapid Response Team on which I served in the immediate aftermath of 9/11 along with Southwest Airlines executive Herb Kelleher and New York Police Department Commissioner Ray Kelly.

Over the past decade, AAAE and individual airports have worked closely with TSA and the technology community to implement specific programs, including Registered Traveler. In roughly one year, the RT program enrolled more than 250,000 travelers at 24 airports, proving the security and efficiency benefits that adoption of these programs provides.

Although not directly responsible for processing passengers at screening checkpoints, airports long ago recognized that there was great potential value in terms of enhanced security and efficiency with the deployment of trusted traveler programs. Airports have also understood that they are uniquely situated to bring interested parties together to chart a course that would result in the successful deployment and operation of the program.

With more than 700 million passengers traveling through the U.S. aviation system each year – a number that is expected to grow significantly in the years ahead – it is high time that efforts are made to make the promises of a trusted traveler program a reality, and we are pleased that TSA is moving in that direction. A small percentage of frequent air travelers take almost half of the trips through the aviation system, and we should make every effort to provide a different screening protocol for this group. Doing so will help expedite the screening process for all travelers and allow screeners to focus more intensely on unknown and potential threats.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01302 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.883

AAAE Supports TSA's Risk-Based Approach to Passenger Screening
Airport executives are encouraged by the recent efforts of TSA to move forward with the PreCheck program, a limited, voluntary passenger pre-screening initiative with a small trusted/known traveler population at four airports. Administrator Pistole and his team deserve immense credit for moving forward with the program and with other risk-based initiatives. As I mentioned, airports have long been supportive of the trusted traveler concept that underlies the PreCheck program, and we are eager to work with TSA to expedite the adoption of the program on a wide-scale basis beyond the initial populations and airports.

Airport executives anticipate great success with the PreCheck program and recognize that the next challenge will be moving from a largely airline-centric program in operation at a handful of airports to one that is operational for large numbers of travelers at airport facilities across the country. Airport operators are uniquely situated and qualified to play a key role in assisting TSA in efficiently and effectively growing participation in PreCheck or a similar trusted traveler program. AAAE has established a Security Task Force that is actively involved in discussions with the agency to move in that direction, and we are optimistic those discussions will produce tangible results soon. The group is also working collaboratively with TSA to address issues related to checkpoint configuration, queue management, modified LEO response expectations and public communication.

Airports are confident that in partnership with TSA they can help facilitate the deployment of a robust trusted/known traveler program that focuses on enhanced security above all else in addition to expediting the travel experience. These two pillars are the primary values that the nation's frequent air travelers want and that each of you as policymakers rightly will demand. By bringing efficiency back into the nation's airport screening checkpoints, TSA screeners will be able to better focus their limited resources on the critical task of providing more rigorous screening to individuals about whom we know less than those who use the system the most and have voluntarily submitted background information for extensive vetting and clearance.

Public/Private Partnership and Collaboration Facilitate Enhanced Security
While the federal government obviously plays a leading role with regard to passenger pre-screening and other areas of aviation security, airports and the aviation industry can and should play an active role in partnering with the federal government to design and implement meaningful solutions to security challenges – at checkpoints and throughout the airport environment. The establishment of effective public/private partnerships has already proven extremely successful, for example, in building a system for processing fingerprint-based background checks and additional background screening for more than eight million airport and airline employees through the Transportation Security Clearinghouse. I have included a fact sheet on the TSC at the end of my testimony for the Committee's review.

Additionally, we are encouraged by recent efforts by TSA to enhance cooperation with airports on the policy and operational front, including the work of the In-Depth Security Review. The IDSR, which was recently recognized for a TSA Partnership Award, is a collaborative effort between TSA, AAAE, and other aviation interests to review Security Directives and other requirements and provide recommendations on measures that can be updated, rescinded, or consolidated into Airport Security Program amendments.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01303 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.884

The IDSR effort has made significant progress in addressing specific areas of concern and stands as a model for collaborative efforts going forward to ensure that policy and operational changes are made in consultation rather than by emergency regulation or directive. In our view, the security interests of the nation are best served when the federal government, local governments, and affected parties work in concert to address outside threats.

Airport Credentialing and Access Control Should Remain With Local Airport Control
While airport executives are encouraged by many ongoing initiatives within TSA, we do have concerns about efforts to "harmonize" or "modernize" various aspects of existing transportation worker vetting programs. In the aviation environment, the background check process for workers operates successfully as a federal/local partnership with the federal government holding sole responsibility for security threat assessments and other necessary government checks for prospective workers and with local airport authorities operating and managing enrollment, credentialing, badging, criminal history background check adjudication and access control systems in accordance with strict federal standards.

The current system for aviation ensures the highest level of security by combining the unique local experience, expertise, and knowledge that exists at individual airports with federal standardization, federal oversight, and federal vetting assets. Local involvement provides a critical layer of security and gives airports the operational control they require to ensure that qualified employees receive the credentials they need to work in the airport environment.

In contrast to the long-standing locally controlled credentialing and access control apparatus that exists in the aviation environment, the credentialing/access control system in place in the maritime environment with the Transportation Worker Identification Credential (TWIC) program is relatively new. Under the TWIC model, the federal government or its contractors are responsible for virtually all aspects of the process, including worker enrollment, applicant vetting, credential issuance and some elements of access control. In our view, the early results of TWIC have been uneven at best despite hundreds of millions of dollars in federal investments. The existing system in aviation operates at no cost to the federal government.

Some have suggested abandoning the successful local systems and processes already in place at airports with badging and access control to expand TSA and the federal government's control over more of the process as is the case with TWIC in the maritime environment. Airport executives oppose any move to shift any additional functions in aviation to the federal government and believe that such a move would diminish security by reducing or eliminating a critical, extra layer of security that is already in place in airports and absent with the TWIC approach.

Pursuing such an approach would scuttle a successful local/federal model that has worked well for decades, eliminate local operational control, stymie significant efforts already under way at airports across the country to upgrade and biometrically enable existing airport badging and access control systems, and significantly increase costs to the aviation industry with no demonstrable security benefit.

While the desire to centralize and federalize the process for all transportation worker vetting programs in the name of modernization or harmonization may be understandable from the federal government's perspective, airport executives are concerned about federal intrusion into

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01304 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.885

existing processes that have worked well for decades. Airports are also very concerned about having to help foot the bill for these initiatives – estimated at $571 million through 2018 as part of the TTAC Infrastructure Modernization (TIM) program – for changes that provide them with no demonstrable security or operational benefit. The current system in aviation operates efficiently and effectively at a fraction of the cost of other transportation vetting programs and at no cost to the federal government. We want to ensure that remains the case.

Rather than discarding the successful, local systems and processes already in place at airports with credentialing and access control and expanding the agency's already daunting mission, TSA should focus its efforts on improving its own vetting systems. TSA can and should continue with its efforts to modernize and harmonize its internal vetting programs without the need to expand the federal government's responsibilities to include credentialing and access control. Congress should make clear that those responsibilities must remain with local airports as has been the case for decades.

Biometric Airport Security Identification Consortium (BASIC)
Before concluding, I want to take this opportunity to bring the Committee up to date on a related topic and the efforts of the Biometric Airport Security Identification Consortium or BASIC initiative. In simple terms, the objective of BASIC is to define a comprehensive, airport-driven Concept of Operations that will enable voluntary migration to biometric-based badging and access control systems at airports. More than 40 airports of all sizes actively participate in BASIC, working cooperatively with TSA and other groups.

Many airport operators are eager to move forward with biometrics, but concerns remain about the prospect of overly prescriptive and costly solutions. Airports are also eager to avoid repeating mistakes made in the past where the federal government required costly and often proprietary access control systems to be deployed in airports in a short period of time. That approach proved both expensive and ineffective.

In an effort to avoid unnecessary regulations and a one-size-fits all mandate regarding biometric-based systems, airports participating in BASIC have identified several key principles that must be part of any future biometric-based badging and access control systems, including:

- Safeguards on local control and issuance of credentials,
- Leveraging of existing capital investments and resources,
- Standards-based open architecture and local determination of qualified vendors, and
- Phased implementation that migrates over time

In addition to building on the processes and regulations already in place at airports today, BASIC is also working to adapt important federal standards regarding secure biometric credentials into the airport's operational environment. For example, Federal Information Processing Standard (FIPS) 201 and the more recent Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers are reflected throughout the BASIC Concept of Operations and greatly inform the recommended phased implementation for airports.

The BASIC working group, which meets on a regular basis, is moving forward aggressively to develop a detailed Concept of Operations that will define the biometric components and common business processes that need to be added to airports' existing procedures to enable biometric-

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01305 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.886

based badge and access control systems in a reasonable and cost-effective timeframe. In fact, several airports have already begun to implement the early phases of the BASIC Concept of Operations. Newark Liberty International Airport, San Francisco International Airport, Aspen Pitkin County International Airport, Los Angeles International and Salt Lake City International Airport – to name just a few – have implemented a secure messaging structure for the submission of biographic security threat assessments and biometric criminal history record checks that will ultimately enable the return of trusted biometrics back to the airport for use on credentials or in access control systems.

Airports are committed to moving forward to bring biometrics into the airport environment as soon as possible in a manner that builds upon existing capabilities and limits operational difficulties. The BASIC initiative, which is being driven by airports in cooperation with the federal government, offers the best opportunity for making the promises of biometrics a reality in a timely manner.

Conclusion

Mr. Chairman, while challenges and frustrations remain on the security front, the experiences of the past decade have both dramatically increased security and left industry and the federal government better equipped to meet future challenges and opportunities. Airport executives look forward to working closely with TSA and the Congress to ensure that limited federal and local resources are used as effectively as possible to ensure the safety and security of the traveling public.

I appreciated the opportunity to be here today and look forward to any questions you have.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01306 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.887

TRANSPORTATION SECURITY CLEARINGHOUSE

Enhancing Security and Aviation System Efficiency at No Cost to the Federal Government

TRANSPORTATION SECURITY CLEARINGHOUSE

What is the Transportation Security Clearinghouse and Why was it Created?

Prior to 9/11, aviation workers were required to undergo fingerprint-based criminal history background checks (CHRCs) conducted by the FBI in any instance in which they could not show a 10-year history of continuous employment. The checks were processed by the federal Office of Personnel Management and routinely took weeks to complete, averaging over 50 days for a prospective employee to receive background check results. Those delays kept airport and airline employees from their jobs for extended periods of time while they awaited required checks, imposing a heavy burden on airport operations and employees.

Following 9/11, Congress required that all aviation workers – some one million workers as opposed to the much smaller subset of workers with a break in continuous employment – undergo fingerprint-based criminal history record checks within a year. Recognizing that this important mandate could not be met utilizing the OPM-run process in place at that time, the American Association of Airport Executives created the ***Transportation Security Clearinghouse*** (TSC) in partnership with the federal government to process the required background checks for aviation workers. The TSC established a high-speed, secure method to collect employee fingerprints for more than 500 airports and multiple airlines across the country for FBI checks, reducing processing times to a matter of hours rather than weeks – and ensuring that the congressional mandate for worker checks was met. Since its establishment, the TSC has processed more than eight million records for vetting against federal criminal history and terrorist data bases.

In addition to facilitating aviation worker CHRCs, the TSC has been instrumental in ensuring that a subsequent TSA mandate to conduct biographic-based security threat assessments (STAs) for workers in and around the aviation environment was completed in a timely manner without major disruptions to airport or aviation system operations.

The TSC: A Record of Success at No Cost to the Federal Government

Of the transportation worker vetting programs in existence today, the TSC stands out as a model of success in terms of security benefits achieved; the number of employees vetted; the cost per worker for vetting; costs to the federal government; record processing time; and the error rate for record submissions. **The TSC has built its unparalleled record of success at absolutely no cost to the federal government,** a remarkable fact considering the hundreds of millions of dollars that the federal government has spent to build similar background check programs for port workers and hazardous material truckers. The TSC provides:

- ***Exceptional Security:*** The TSC has facilitated the vetting of more than eight million records against federal criminal and terrorist data bases with less cost, implementation time and quicker results than any other comparable vetting program of its kind at **no cost to the federal government**. The TSC is routinely audited by TSA to ensure that it meets federal requirements for data protection and other strict federal standards. In addition to its benefits to the aviation industry, the TSC has served the federal government by enabling TSA to quickly implement evolving security requirements, including Security Threat Assessments for all aviation workers, with minimal disruptions.

- ***Low Costs/Millions in Industry Savings:*** Cost per aviation employee is roughly one-third what port workers and hazardous material truckers pay. Cost reductions and enhanced process efficiencies that have minimized employee time spent waiting for background checks and away from their jobs have resulted in hundreds of millions of dollars in cumulative operational savings.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01307 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.888

AIRPORTS COUNCIL INTERNATIONAL

Testimony of Gregory Principato
President
Airports Council International-North America

Submitted to the

Senate Homeland Security and Governmental Affairs Committee

"Ten Years After 9/11: The Next Wave in Aviation"

November 2, 2011

Airports Council International-North America
1775 K Street, NW, Suite 500
Washington, DC 20006
(202) 293-8500

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01308 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.926

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for providing Airports Council International – North America (ACI-NA) with the opportunity to explain our views of our nation's aviation security system and its technology. Airports Council International – North America's 344 member airports enplane more than 95 percent of the domestic and virtually all of the international airline passenger and cargo traffic in North America. More than 350 aviation-related businesses are also members of ACI-NA, providing goods and services to airports.

Coordination with Airports

There is a tendency to view aviation security in isolation without fully considering the impact of our requirements on foreign countries, and in particular, their airports. For example, the Transportation Security Administration (TSA) imposed additional security requirements on domestic and international airlines with flights to the United States after the attempted terrorist attack on Christmas Day in 2009. As these new security measures were being implemented, many flights were delayed and passengers endured significant wait times at security checkpoints, especially in Canada. Although the Department of Homeland Security (DHS) and TSA coordinated closely with the airlines in the immediate aftermath of the attempted bombing, it did not coordinate as effectively with airports and the impact of the enhanced passenger screening requirements – particularly at Canadian airports – was significant.

Although DHS Secretary Janet Napolitano had several meetings with airline representatives and their associations after the Christmas Day bombing attempt, there was little coordination or information sharing between DHS and the airport industry. In a meeting requested by ACI-NA with Secretary Napolitano, ACI-NA offered to assist the Secretary in identifying sustainable aviation security measures through the International Civil Aviation Organization (ICAO), given that Airports Council International (ACI World) serves as the officially accredited airport representative to ICAO.

Since that time, DHS and TSA have worked extensively with foreign governments and through ICAO to strengthen aviation security standards and encourage the use of the latest screening technology. As a result of these efforts, ICAO issued a Declaration on Aviation Security which recognizes the need to strengthen aviation security world-wide through the uniform application of aviation security standards and available screening technologies while putting a priority on the research and development of explosive detection technology. Working closely with our international partners and all industry stakeholders to share the latest available intelligence information will best position government and industry to address the global aviation security challenge in a way that ensures the appropriate level of security while streamlining the process for our passengers now and into the future.

Technology

While there have been significant advances in the research and development of cutting edge passenger and baggage screening technologies, a cohesive screening technology research and

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01309 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.927

development plan that leverages government and industry expertise has yet to be formulated. With the significant focus on screening passengers and baggage, the development of next generation screening technology, including air cargo screening technology, has suffered and should also be a priority. The development of next generation security technologies could be initiated more efficiently through government-administered grant programs that provide incentives to manufacturers.

In order to minimize operational disruptions to the greatest extent possible, it is essential that TSA develop a recapitalization plan for explosive detection systems (EDS) in close coordination with airport and aircraft operators. Almost half of these systems deployed at airports to screen checked baggage in the years after September 11th, will reach the end of their useful lives by 2013, and two-thirds of those systems within the next five years. To address the need for replacement or "recapitalization" of these systems, TSA is in the process of developing a strategic plan that will prioritize the recapitalization of EDS systems based upon their operational reliability.

We routinely encourage TSA, the European Union (EU) and other countries to collaboratively develop mutually recognized detection standards for security screening technology. The identification of mutually recognized detection standards will allow manufacturers to develop screening technologies that can be used in different countries while stimulating competition between manufacturers, resulting in technology enhancements and lower costs. Further, the deployment of screening technology developed in accordance with such standards will allow passengers, baggage and cargo to be screened once, thus paving the way for true harmonization, something that is essential to further enhance the efficiency and effectiveness of the security process, especially as we prepare for the anticipated increase in the number of passengers in the coming years.

For example, inter-governmental coordination could readily address the current process of re-screening connecting baggage from Canada at U.S. airports. This requirement is redundant and unnecessarily drains limited TSA and industry resources as the checked baggage has been inspected by U.S. Customs and Border Protection (CBP) officials, is screened prior to departing Canada, and has flown at least one segment upon arrival in the U.S. TSA should work with the Canadian authorities to develop mutually agreeable checked-baggage screening procedures or technologies at Canadian airports, which would eliminate the need for re-screening at U.S. locations. This would not only free up limited TSA resources but also reduce the operational burden on airports, decrease flight delays and minimize the amount of misconnecting checked baggage.

Finally, while biometric employee identification and access control offers some potential security benefits, implementation is very costly and should not be the result of an unfunded federal mandate. While a few airports have begun to test and install biometrics in accordance with existing TSA technology standards, a federally-funded pilot program is necessary to evaluate the capabilities of biometric employee identification and access control. Subsequent to a

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01310 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.928

pilot test, results must be scrutinized to determine which systems should be included on a government-developed qualified products list. In consideration of the limited availability of resources, funding must be provided to airports for the installation of biometric employee identification and access control systems.

Risk-Based Security and Trusted Traveler Programs

We must continue to shift from a rigid process of screening for bad things to a system that draws upon the vast amount of available data to focus the most invasive security processes on bad people. A risk-based system is absolutely what is needed and TSA should be applauded for its initiative to embark on several risk-based security initiatives and pilot programs involving pilots, passengers and cargo.

ACI-NA supports TSA's PreCheck known traveler pilot program. From a practical perspective, this risk-based program harnesses available data – provided by passengers on a voluntary basis – and intelligence information to serve as an indicator to guide the application of screening resources. By redirecting more rigorous resources to individuals about which the least is known, this streamlines the screening process and reduces traveler frustration.

ACI-NA also supports the CBP's successful risk-based Global Entry program and encourages the Committee to support CBP in its expansion to additional U.S. airports, thus enhancing facilitation and security for all participating passengers. Global Entry has reduced average wait times for enrollees by more than 70%, and this is crucial in helping to leverage limited CBP resources during busy travel seasons, when passenger demand increases significantly. Expanding Global Entry to additional airports and airport terminals will increase the value of the program to enrollees and thus promote increased enrollment, benefitting all passengers, the aviation industry and CBP.

TSA has partnered with CBP to allow members of existing international trusted traveler programs, Global Entry, SENTRI and NEXUS, to participate in TSA's PreCheck known traveler pilot program. Airports in the United States and Canada are very supportive of these risk-based international trusted traveler programs that provide the dual benefit of enhancing both security and processing efficiency, since travelers do not have to spend time filling out paper declaration forms. In addition, participating travelers do not have to wait in line or visit CBP officers, thus allowing officers to focus on other travelers. The partnership between TSA and CBP will be essential in expanding current and developing new programs which utilize available data to better focus limited screening resources.

Conclusion

Although there are aspects of the current aviation security system that are effective, there are others which need to evolve to keep pace with the projected increase in the number of passengers and volume of cargo in the United States and abroad. The expansion of risk-based trusted

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01311 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.929

traveler and shipper programs that leverage available data and focus limited screening resources on those travelers and cargo about which the least is known are essential toward ensuring the long-term sustainability of the aviation system. Such programs, which allow the U.S. and other governments the ability to prioritize threats and make adjustments to the security posture based upon credible intelligence information help to ensure limited resources are appropriately focused and allocated.

Although technology provides an essential security layer, it should not be viewed in isolation. Research and development programs should be enhanced by incorporating industry input on operational needs. Existing programs that utilize data to establish risk profiles can be further expanded and networked to focus more invasive technologies and procedures on those travelers and items about which the least is known.

Through continued collaboration, both government to government and government to industry on regulatory, technology and other security initiatives, we can better achieve our mutual goal of enhancing security while minimizing unnecessary operational impacts.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01312 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.930

PRESIDENT'S DEPARTMENT
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL
1625 MASSACHUSETTS AVENUE, NW ☐ WASHINGTON, DC 20036 ☐ 1-888-FLY-ALPA (1-888-359-2572)
FAX 202-797-4007

November 1, 2011

The Honorable Joseph Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Susan Collins
Ranking Member
Committee on Homeland Security and Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Lieberman and Senator Collins:

On behalf of more than 53,000 pilot members who fly for 37 airlines in the U.S. and Canada, the Air Line Pilots Association, International (ALPA) would like to provide you with a synopsis of a number of aviation security concerns that ALPA believes should be brought to the attention of the Senate Homeland Security and Governmental Affairs Committee during its hearing on *Ten Years After 9/11: The Next Wave in Aviation Security*.

Threat-Based Security

The attempted bombing of Northwest (NWA) flight #253 on Christmas Day, 2009 served as a catalyst for ALPA to publish a white paper entitled *Meeting Today's Aviation Security Needs: A Call to Action for a Trust-Based Security System*, in January 2010. In that document, ALPA articulated that the Transportation Security Administration (TSA) needs to change its post-9/11 philosophy of screening all people equally for harmful objects to one that focuses on identifying individuals having evil intent.

We are pleased to acknowledge the positive response from a number of our industry partners, as well as from TSA leadership, expressing agreement with our call for a philosophical change in underlying aviation security philosophy. ALPA has been encouraged by TSA Administrator John Pistole's advocacy for the implementation of more threat-driven, risk-based security procedures, such as a known traveler program, and expanded use of the Screening of Passengers by Observation Techniques (SPOT) program. We are particularly pleased with his public statements that a properly identified and thoroughly vetted pilot flying an airliner should not be required to undergo the same screening procedures as a passenger about whom very little is known. TSA's support for the ALPA-conceived alternative screening program for

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01313 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.931

pilots, referred to as Known Crewmember (KCM), has been a welcome change to previous "one-size-fits-all" screening requirements. ALPA expresses its gratitude to the leadership of the Air Transport Association (ATA) and its member airlines for facilitating the roll-out of KCM.

We believe that significant steps have been taken by TSA to implement more risk-based solutions to securing the aviation sector, and we look forward to continued government and industry partnerships in the expansion of KCM and other threat-based, risk-mitigation programs.

Federal Flight Deck Officer (FFDO) Program

The FFDO program, which uses federally-credentialed, volunteer, armed pilots who are trained and managed by the Federal Air Marshal Service (FAMS) to serve as the "last line of defense" of the flight deck, has dramatically grown since its inception in 2003. The FFDO program has been acknowledged by industry and government to be an extremely successful and cost-effective layer of aviation security. In this era of austerity, the FFDO program's annual budget has remained stagnant since 2004. As a result, TSA/FAMS ceased accepting new applications in 2011 and has announced its inability to accept applications to the program during 2012 as well. Additionally, FAMS is considering certain program cuts to counterbalance the stagnant funding. We respectfully submit that the FFDO program is a cost-effective layer of aviation security and Congress should consider increasing the budget for the program.

Regarding the FFDO program's deployment outside of the U.S., ALPA commends the TSA and the FAMS for their successes to date in this regard, and encourages continued efforts to expand its international capabilities.

Secondary Barriers

On September 28, 2011, design standards for reinforced flight deck door secondary barriers were established by RTCA, a Federal Aviation Administration (FAA)-chartered, standard-setting organization. These inexpensive, lightweight devices are intended to protect the flight deck whenever the reinforced door must be opened in flight. When used in conjunction with appropriate crew procedures, the secondary barrier will assist in identifying and delaying an attacker's intent to do harm. ALPA encourages the use in protecting the flight decks of our nation's airliners to enhance aviation security both domestically and abroad.

Threatened Airspace Management

The failed attack against Northwest Airlines flight #253 demonstrated deficiencies in ground-to-air communications during and after a significant in-flight security event. Pilots in command of other aircraft, either airborne or about to take-off, were not advised in real time of the circumstances impacting NWA 253. This lack of communication deprived these other aircraft commanders, in their role as In-Flight Security Coordinators (ISCs), of critical information

67123.932

which related to a potential security threat to their own flights, and negatively impacted the ability of flight and cabin crewmembers to best protect their passengers and aircraft.

On April 7, 2010, the FAA and TSA did a better job of communicating information to other aircraft regarding an on-going security incident involving a diplomat suspected to be assembling a bomb while in the lavatory of an airliner traveling from Washington, DC to Denver, CO. However, the flight decks of only selected airborne aircraft were notified of the event. Since then, we have not witnessed the sharing of security-related information with aircraft commanders that would be of value to them in fulfilling their duties as pilots-in-command.

As recently as June 19, 2011, a bomb threat was made against a Washington, DC-bound airliner while it was in flight. The captain was not notified of the potential danger until landing at Ronald Reagan National Airport. The aircraft, with its 44 passengers and three crewmembers still onboard, sat on the ground for 29 minutes before emergency responders arrived at the plane and the passengers and crew were allowed to deplane.

In addition to this communications deficiency, we have seen no evidence of a clearly-defined, prioritized plan to control the national air space (NAS) in the event of another 9/11-type attack. The U.S. economy and the domestic aviation industry cannot sustain the negative financial impact resulting from a repeat of a nationwide shutdown as occurred at that time. ALPA urges Congress to ensure the development of a prioritized plan for control of the NAS in such circumstances, with the intent of preventing a total or substantial closure.

All-Cargo Airline Security

In November 2010, law enforcement and intelligence agencies interdicted attempts to bomb two U.S. all-cargo aircraft destined from international locations to the United States. Successful detonation of the explosives, hidden in printer cartridges shipped from Yemen, could have resulted in catastrophic loss of life and the aircraft involved.

These attacks confirmed that all-cargo carriers remain a focus of terrorists. Notwithstanding government and industry awareness of a variety of security vulnerabilities which still exist in the air cargo domain, all-cargo operations remain exempt from a number of security practices mandated for passenger air carriers. Examples include: no hardened flight deck door requirement; no mandated *All-Cargo Common Strategy* training for crewmembers; no requirement for fingerprint-based criminal history record checks for persons with unescorted access privileges to aircraft and cargo; and no uniform requirement for Security Identification Display Area (SIDA) restrictions on all-cargo air operations areas.

Although the *Air Cargo Security Requirements; Final Rule*, published in May 2006, did much to improve the security of all-cargo aircraft and operations, it fell short of the mark in several critical aspects. An investigative report issued by the Government Accountability Office (GAO)

67123.933

on June 20, 2011 provides evidence of a number of these remaining vulnerabilities and bolsters ALPA's argument that much work remains to be done in this regard. Based on the unwillingness of regulators, government and industry to adequately address these deficiencies, we believe that Congressional action is required to bring about needed change.

Laser Illumination of Aircraft

On October 27, 2011 ALPA, in conjunction with the Air Transport Association, sponsored a one-day conference entitled: *Laser Illumination of Aircraft – A Growing Threat.* The event highlighted the very real dangers posed to flight safety by this illegitimate activity which FAA statistics show to be increasing at an alarming rate, and was intended to spur further action to mitigate the problem.

ALPA applauds the FAA's recent announcement of its increased civil fining authority with respect to this activity, up to a maximum of $11,000 per event. We are also pleased the Senate included an amendment in the Federal Aviation Administration reauthorization bill sponsored by Senator Sheldon Whitehouse to make knowingly shining a laser at an aircraft cockpit a federal crime. While we continue to advocate for a multi-year, comprehensive FAA reauthorization bill, we acknowledge the uncertainty of that legislation, and urge the Senate to swiftly pass a stand-alone measure that would make the intentional laser illumination of aircraft a specific federal crime.

ALPA is grateful for the Committee's attention to these critical transportation security matters. We look forward to working with you to better protect the travelling public and the US aviation industry.

Sincerely,

Captain Lee Moak
President

67123.934

AIR TRANSPORT ASSOCIATION

NICHOLAS E. CALIO
PRESIDENT AND CEO

November 2, 2011

The Honorable Joseph I. Lieberman
Chairman, Committee on Homeland
Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20514

The Honorable Susan M. Collins
Ranking Member, Committee on Homeland
Security and Government Affairs
413 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Lieberman and Ranking Member Collins:

On behalf of our member carriers, I am writing to share our views for your consideration as part of your hearing, "Ten Years After 9/11: The Next Wave of Aviation Security." We are committed to continuing to work closely with the Administration to make the aviation security system as secure as possible while facilitating the movement of people and goods domestically and internationally. Our industry depends on efficient and effective security.

We support the Administration's commitment to risk-based screening of passengers, crew and cargo. In the last decade, government agencies with civil-aviation security responsibilities have gained a great deal of experience and data about users of the air transportation system and the threats to that system. This enables well-informed judgments about security risks and the application of finite resources to higher risk situations. Security experts, both in and outside of government, regard this as the most appropriate approach to aviation security.

Along with our pilots, we have partnered with the Transportation Security Administration (TSA) in the "Known Crewmember" demonstration program, which is enabling pilots with the appropriate credentials to undergo a different screening protocol. This risk-based screening enables limited TSA resources to be focused where they are most needed, and reduces security wait times for passengers. We also are working closely with TSA on the PreCheck program for passengers to ensure that we can implement a secure and efficient screening process for known travelers. Finally, we are engaged with both TSA and the Customs and Border Protection (CBP) agency to evaluate a risk-based approach for screening cargo.

The progress we are making toward implementing risk-based screening programs is solid but needs to be expedited. In addition, TSA must begin to realize some of the cost-saving benefits from the efficiencies of these programs, as well as the efficiency savings from new technology. Since 2004, the TSA budget has increased dramatically, despite the fact that the number of people traveling has not similarly increased over the same period of time. What has increased,

75 YEARS OF AVIATION EXCELLENCE
AIR TRANSPORT ASSOCIATION OF AMERICA, INC.
1301 PENNSYLVANIA AVENUE, NW SUITE 1100 WASHINGTON, DC 20004-7202
Phone 202-626-4000 Fax 202-626-4166

however, are the number of new security protocols, including costly and time consuming changes at the checkpoint involving how TSA screens liquids, laptops and shoes.

The Administration has proposed an increase in the aviation passenger security fee, despite the fact that no other industry or mode of transportation is required to pay for federal security. 9/11 was an attack on our economy and the entire U.S. population, not on the airline industry or our customers. National security is in the national interest, and the costs associated with defending the country against terrorism should be borne by the federal government.

And yet now, the Administration is proposing tripling that tax. U.S. airlines and their passengers contributed $3.7 billion in taxes and fees to the Department of Homeland Security (DHS) in FY2011 – a 50 percent increase from the amount collected in 2002. The industry's federal tax burden on a typical $300 domestic round-trip ticket has nearly tripled since 1972, from $22 to $61. As a result, aviation security taxes and fees now constitute almost 23 percent of the industry's federal tax burden.

To put this tax into perspective, the U.S. airline industry's total profit last year was $3.7 billion, one of only three profitable years over the last decade – a decade in which U.S. airlines lost $55 billion and shed nearly 160,000 jobs. Further increasing our tax burden will exacerbate this problem and further undermine the industry's financial health, thereby undermining the overall economic recovery.

Finally, we believe that TSA should continue to work with its foreign civil-aviation security counterparts to mutually recognize security practices. This will eliminate air carriers from being subject to multiple security regimes at overseas locations. Such overlapping regulatory requirements do not enhance security. Harmonized requirements, in contrast, do advance security and efficiency.

Effective, efficient security is vital to the U.S. airline industry in fulfilling our central role in propelling commerce and the economic vitality and global competitiveness of our country. With these facts in mind, we urge you to reject any increase in the passenger security tax.

Sincerely,

Nicholas E. Calio

STATEMENT OF

MARCUS W. FLAGG, PRESIDENT
FEDERAL FLIGHT DECK OFFICERS ASSOCIATION

Before the

COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENT AFFAIRS

Hearing on
"Ten Years After 9/11: The Next Wave in Aviation Security"

November 1, 2011

Chairman Lieberman, Senator Collins, Members of the Committee, I am pleased to provide testimony before you this afternoon on the hearing "Ten Years After 9/11: The Next Wave in Aviation Security". My name is Marcus Flagg and I am a United States Naval Academy graduate, a former Navy fighter pilot and a graduate of the Naval Post-Graduate School on Aviation Safety. I am also currently an airline pilot with UPS Airlines. On September 11, 2001, my father RADM Bud Flagg USNR and my mother Dee Flagg died aboard American Airlines flight #77, when it was commandeered by terrorists and crashed into the Pentagon.

Since 2001, I have been proactive in improving aviation security to help protect our country against terrorism. I currently serve as President for Federal Flight Deck Officers Association (FFDOA), a not-for-profit and non-compensated trade association. FFDOA represents Federal Flight Deck Officers (armed pilots), which now represent the Fourth largest Federal Law Enforcement organization in the United States. The FFDO program is an extremely viable, cost effective, and successful element of our national aviation security effort today.

SECURITY PHILOSOPHY

I believe in integrated security solutions that work together as a "system of systems" providing the maximum deterrent against terrorist attacks at the lowest possible expense. Flight crews are a key element in an integrated security system and are an asset that has yet to be fully exploited. Aircraft on the ground should be protected with security measures that begin in the cockpit and radiate outward to the airport parking lot and beyond. This clearly requires the cooperation of several different entities. Once a flight is airborne, only on-board assets can affect the positive outcome of a security breach. Therefore, it is crucial that flight crews have the training and information necessary to influence a safe outcome. The lives of hundreds of innocent Americans on-board the aircraft and thousands on the ground hang in the balance. Nothing can be made terrorist-proof, but intelligent and coordinated programs can provide a powerful deterrent to those who might attack the aviation interests of our country.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01319 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.937

COCKPIT DEFENSE

Federal Flight Deck Officers (FFDOs) are the first line of deterrence and the last line of defense. This is the most cost effective security measure we have to date. FFDOs are trained to stop a threat using the full spectrum of the force continuum. While the training is consistently reported as excellent, serious questions remain about the Transportation Security Administration's (TSA) administration of the program. In 2002, the entire TSA, from the Administrator on down was adamantly opposed to the FFDO program. The current TSA Standard Operating Procedure (SOP) and Sensitive Security Information (SSI) was written during that time frame. Historically, the TSA has been problematic in restricting FFDOs as much as possible. Many of the individuals from that era are still in key positions. The current TSA needs a top down review and reorganization to meet challenges and threats that our country faces. The FFDO program is a growing federal officer corps, but many more pilots are needed. Those volunteers will not be forthcoming unless fundamental changes in duty firearm carriage, liability, time for training without airline obstruction, and international flight coverage are made to the program.

Officer safety should be the top priority and equal to the safety of passengers. No law enforcement officer handles a duty firearm as many times a day as does an operating FFDO complying with the TSA SOP. The requirements of the onerous FFDO SOPs are a formula for an accidental discharge. The present duty weapons transport protocol will lead to the loss of duty firearm retention, and directly contradicts sound law enforcement practices. The lack of significant incidents related to the current FFDO SOP is more indicative of superior performance of FFDOs than well constructed policy.

The politicizing of FFDO procedures and defiance of law enforcement lessons-learned places FFDOs and others in the airline environment at risk, as well as poses a liability on many fronts. FFDOs should be allowed to transport a locked duty firearm as an option, but otherwise carry their duty firearm on their person. Removing Section "G" completely from the Armed Pilots Against Terrorism Act (APATA 2002) would allow Portal-to-Portal concealed duty firearm carriage. This small but significant change would dramatically increase pilot participation in this viable and highly effective program.

A FFDO as a flying pilot at the controls would defend the aircraft from the cockpit only, and not exit the cockpit. If one or more FFDOs are riding as passengers in the back of that same aircraft, they may be the only trained law enforcement on board (including cockpit crew). They should not be restrained by the government from defending the cockpit in the event of a terrorist attack regardless of the side of the cockpit door they are seated, as they are now. The absence of this element of the program is very damaging on more than one front.

On September 11th, a Federal Officer was on board United Airlines flight #93. Unfortunately, because of the FAA and his agency policy, he had to check his weapon as baggage in the belly of that aircraft. Threat assessment aside, the inability to operate internationally translates into many FFDOs who may not operate domestically, since they fly mixed domestic and international flying schedules. This takes trained FFDOs out of the system.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01320 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.938

Currently, FFDOs provide five times the coverage of the Federal Air Marshal Service at 1/25th the cost. The cost of each Federal Air Marshal is around $3,300 per flight. A pair of FAMs cost roughly $6,600 per flight. FFDOs cost roughly $15 per flight. Comparing the two, the same expenditure allows 440 FFDO missions to the single FAM mission. Which program is more cost effective?

Cabin crewmembers properly employing defensive tactics could provide cockpit crews with critical time to prepare a cockpit defense plan and land the aircraft. Currently, the TSA has developed a voluntary Crew Member Self Defense Training (CMSDT) program that all crewmembers may take as often as they like. A volunteer program that requires crewmembers to pay for their own travel and hotel expenses on their own time, mitigates the value of this excellent course.

The cabin crew should also have a remote means of communicating with the cockpit crew in the event of a security breach, in addition to their present antiquated primary and secondary communication methods. The Airline Transportation Association (ATA) lobbying efforts defeated legislation mandating such a system. The ATA also lobbied against installing cameras in the cabin of passenger airliners, a method to help provide the cockpit crew with vital situational awareness in the cabin. These systems cost less than the entertainment systems that many airlines have installed.

The Federal Air Marshal (FAM) program, although another excellent layer of security, has serious shortcomings. The Federal Air Marshal Service also manages the current FFDO program. FAMS and FFDOs should be separate and equal divisions operating under the TSA Office of Law Enforcement. An immediate available additional improvement to this viable program would be more involvement and cooperation in training between FAMs and FFDOs. This would require additional funding to support and train the FAM/FFDO team concept. Presently, FAM Field Offices cannot accommodate FFDOs who wish to use the FAM facilities to improve their skills and teamwork.

Of all the proposed aviation security enhancements available today, "flight deck secondary barriers" represent the single most effective additional layer to help protect the flight deck with FFDOs from another potential hijacking. Congress mandated the installation of flight deck hardened doors in 2001, but at the time didn't anticipate the need for a secondary barrier. FFDOA and almost every other industry group have since come to the conclusion that a hardened door alone does not provide a predictably reliable barrier to an attack. In order to protect the flight deck effectively during times that the door is opened in flight, the crew needs a protected space in front of the flight deck door, and a few seconds to respond to an attempted breech.

Secondary Barriers, such as those currently installed on some of United Airlines airplanes, provides crews the essential space and time to accomplish a door transition. Secondary barriers are extremely inexpensive when compared to other security systems, are easily installed, and can be easily incorporated into current flight deck access procedures as modeled by United Airlines and other carriers. Most importantly, like the mandated hardened flight deck doors, a Congressional mandate of secondary barriers would result in a significant layer of aircraft security in minimal time.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01321 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.939

In order to expedite this security enhancement Congress should fund the cost of installing secondary barriers, including reimbursement of carriers who are already beginning to install this much needed aviation security enhancement through tax credits for each secondary barrier installed.

A major problem for all three layers of security is that there is no integration of training, or at the least, a clear understanding among each group on how to work together. These three systems have been "stove piped." In addition, the TSA does not require crewmembers to receive operational Security Directives. The TSA provides this information to airline corporations and lets them decide who the "need to know" employees are. Very few airlines have chosen to share this vital information with cockpit and/or cabin crews. A notable example of the failure to disseminate information to airline crews was the Richard Reid "shoe bomber" incident.

Previously, crewmembers were not told of an existing threat to passengers involving explosives in shoes. It was not until after this event that American Airlines elected to change their policy. Other airlines provide only a minimal and cryptically scrubbed version, usually in an untimely manner. It is unconscionable that the TSA leaves this crucial information to individual airline policy and does not require delivery of the operational information to pilots and cabin crews.

CARGO SECURITY

Dramatic growth and maturity for the all-cargo airline has occurred over the past 30 years. In their earlier days these airlines were not very big, and operated at night beyond the view and consciousness of the general public. Today, they are large global airlines that operate around the clock, flying the same aircraft in the same flight environment as the passenger carriers do.

For years all-cargo airlines were exempt from many of the government safety and security regulations required of passenger carriers. One such example involves a critical airborne Traffic Collision Avoidance System (TCAS) that was required of passenger aircraft, but not mandated on cargo aircraft until 13 years later. This lack of uniform safety standards continues today as illustrated by their being no requirement for airport Aircraft Rescue and Fire Fighting (ARFF) to be provided for the all-cargo aircraft, nor for the first responders to conduct any training on all-cargo aircraft. Hardened cockpit doors are non-existent on cargo aircraft, although mandatory on passenger aircraft.

All-cargo aircraft do not have FAMs nor LEOs aboard the aircraft, nor around the aircraft to prevent a hostile takeover. Hardened cockpit doors should be mandatory on all current and future all-cargo aircraft. All-Cargo carriers routinely receive exemptions from government regulations imposed on passenger carriers. Unfortunately, this same double standard is placing all Americans at risk.

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01322 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.940

A new Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP) does mandate security training to crewmembers of all-cargo airlines. However, the original requirement was reduced by fifty percent at the request of the Cargo Airline Association (CAA) and ATA and is clearly insufficient in regards to training initial crewmembers. Many all-cargo airline corporations have fought against the training for their pilots claiming the cost is too great. When pilots have petitioned their companies to work with them to develop programs, airline managers have told them they would refuse to incorporate such training unless the government mandates it. It would seem obvious that an all-cargo B-767 can cause just as much damage as a passenger B-767, whether hijacked or detonated over a populated area. This is a fact that has been lost on airline managements having a pure economic bias, and keeps them rooted in the old ways of doing business, hoping nothing will happen again, and believing they are not responsible for security.

Airport security standards have seen minimal enhancement for the all-cargo operation. While minor improvements are underway for larger airports, many smaller airports are not required to have an airport security program, and are still not required to make any changes even though they host large jets and are located near major populated areas. Once again the excuse given is the fear of "financially overburdening" the all-cargo airlines. Additionally, the TSA does not want to establish new rules that may be difficult to understand by people that never had to follow them at unregulated airports.

The recent attempted "toner cartridge bombing" on FEDEX and UPS aircraft illustrates the need to screen all cargo on all-cargo aircraft as well as passenger aircraft.

I believe in "*One Level of Security*" for cargo on passenger and all-cargo aircraft.

CREW SCREENING

Physical screening of crewmembers prior to flight is conducted as part of the TSA program for providing airport and flight security. Designed to prevent another 9/11-type attack, this method of screening crewmembers is ineffective and wastes resources. Legitimate crewmembers must have access to aircraft in order to fly them, and therefore do not require a screening routine designed to stop potential terrorists at the passenger screening portal. Therefore, for crewmember screening to be meaningful, the process must be able to confirm or deny the identity of an individual as a crewmember so as to prevent unauthorized access. The Known Crewmember Screening System was introduced this year to address this problem, but is stuck in a painfully slow testing phase, with limited locations, and currently excludes cabin crewmembers without justification.

PASSENGER SCREENING

FFDOA recognizes the nature of a changing threat, and the necessity for a proactive approach to mitigate that threat. There are solutions for passenger screening that rely on physical security, technology, and the human element. FFDOA believes that the TSA has

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01323 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.941

made large investments in time and money building a system that looks for dangerous "things" instead of dangerous people. We are convinced that this approach is fundamentally flawed.

The current state of passenger screening in the United States has made some limited improvements over the screening methods used pre-9/11. More "process" has been added in an effort to create a serious, but not necessarily more meaningful, screening environment. The selectee process is significantly flawed and the secondary screening provides little if any advantage over the initial primary screening.

A new expedited screening program allows U.S. citizens who are members of the U.S. Customs and Border Protection (CBP) Global Entry, NEXUS, and SENTRI Trusted Traveler programs to participate in this TSA pilot program. TSA should focus resources on higher-risk and unknown passengers while expediting the process for lower-risk and known passengers whenever possible. There is a system that exists that would provide a dramatic improvement in anti-terrorism mitigation, and provide an additional bonus of customer satisfaction. It is known as Behavior Pattern Recognition (BPR).

The TSA currently uses a trimmed-down version of BPR called Screening Passengers by Observation Techniques (SPOT). The SPOT program only teaches TSA Security Officers how to detect one of three main elements that make BPR work. The other two elements are delegated to the airport law enforcement officers, who clearly are the backbone of airport security. As trained law enforcement officers, they have the bearing, temperament, and most importantly, the authority of law to conduct this important security feature, although they are not presently required to receive BPR training. If the full BPR were to be used by TSA Security Officers as a major screening method, experts report that selectee counts would be reduced from the current high numbers, down to a very low percentage. Additionally, that significantly smaller number would receive a more thorough and meaningful secondary screening than presently exists. This serious, behavior-focused program is specifically designed to look for traits exhibited by those with threatening intent.

Pilots and flight attendants are excellent candidates to receive training in the SPOT or BPR program since the majority of their time is spent within the airport environment. Once again, this is an untapped potential that TSA has chosen not address. At the passenger screening portals, the ability to keep threatening intentions and material, such as explosives, off the aircraft cannot depend on the current x-ray machines and TSA screeners alone. Chasing every tool a terrorist may use is sadly ineffective.

As we look at technology, we recognize it has a necessary and evolving role in the passenger screening effort. A properly-run BPR program in combination with K-9's, or their technological equivalent (such as fluorescent polymer), can be very effective at mitigating many types of "carry on explosives" and other threat behavior; "looking for bombers, not for bombs is a better approach". Magnetometers, or metal detectors, have been staples of passenger screening for decades. Both walk-through portals and hand wands continue to be

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01324 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.942

useful tools, but portals are also becoming enhanced to trace explosive detectors. The use of x-ray technology can be added to these portals, but many passengers have privacy concerns over the display of their body images. These images can be "cartooned" so actual body types are not displayed.

Screening devices for carry-on bags have enhanced features (that have been in place for many years), but the government is preparing to further enhance these units with existing bomb detection technology. Detectors are in development for liquid explosives, but they are presently too slow and lack sufficient accuracy. Bomb sniffing dogs (K-9s) have their limitations, but are very accurate, and also serve as an outstanding interim fix while we wait for future technologies currently in development. Closed Circuit Television (CCTV) is a good tool for tracking and documenting activity in the entire airport environment, from the parking lot to the airplane.

Physical security is being adjusted at many airports. This will be an essential design feature for future airport projects. Parking lot locations, terminal stand-off features and materials, as well as electronic "one way" gates to help prevent portal breaches, will be among the approaches the physical security element affecting passenger screening.

MANPADS

Man Portable Air Defense System (MANPADS), otherwise known as shoulder-fired missiles, pose a clear threat to commercial aviation. Over the past twenty years, numerous aircraft have been fired upon by MANPADS in countries outside the U.S. The proliferation of MANPADS has escalated to the point that there is now serious concern of an attack in the United States.

Economic realities may prevent retrofitting the entire U.S. airline fleet with the most expensive MANPAD countermeasures. Of primary concern is the Civil Reserve Airline Fleet (CRAF). These large jets are U.S. registered airliners (both passenger airlines and all-cargo airlines) that fly in support of our U.S. troops abroad. At present, they are the most vulnerable, and should be outfitted first. Also, different manufacturers provide different successful solutions. MANPADS is not an airport perimeter issue. The operating envelope of this weapon system could enable an attacker to be "away" from the airport environment.

TSA

It has been over ten years since September 11th. The TSA was formed to standardize aviation security. This is not the case. Each airport is its' own domain, isolated in its' exclusive security plan. Consistency throughout the system is non-existent. Pilots, crewmembers and FFDOs should be treated uniformly and consistently throughout the system. We are either the problem or the solution, we cannot be both. The TSA also labels everything SSI to hide

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01325 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.943

their problems and shortcomings. FFDOs and the FFDO program office cannot communicate with other FFDOs nor call FFDOs FFDOs, but rather pilot volunteers. These obtuse SSI restrictions now place the mission in jeopardy by muzzling FFDOs.

Past TSA congressional testimony always claim credit for working towards solutions, but is shallow on achievement. Why? Because the TSA has ceded its' authority to allow the airport security directors to run the show. Additionally, the TSA has become an inflexible bureaucracy, resistant to new ideas from stakeholders. Meetings and working groups are used to reinforce their existing policies and to placate the GAO reports. TSA is a reactive regulatory agency unwilling to provide proactive changes. TSA officials, for the most part, do not have an aviation background nor do they understand the industry they are attempting to protect.

SUMMARY

Aviation continues to be the favorite target of terrorists. This threat is real and evolving therefore we must stay one step ahead of the terrorists. Any attack on aviation would ground the nation's airline fleets with a resulting economic impact estimated by the Department of Transportation to be $10 billion U.S. dollars per week. This figure, of course, does not account for the potential tragic loss of human life in the air and on the ground.

Pilots and cabin crews are active participants in aviation security and will live and die by TSA's decisions and policies. Every day, pilots and cabin crews operate in an environment with no margin for error. Since man began flying, aviation has been inherently dangerous, and today's airline pilots know that the FAA rules and regulations are all written in blood.

Many resources from various elements of security must work together to mitigate a terrorist threat. In the event of terrorist action, once airborne, the only viable resources are the ones on the aircraft.

Chairman, and members of the committee, I thank you again for the opportunity to provide testimony today. I am happy to respond to any questions that the committee may have.

Respectfully submitted,

/s/
Marcus W. Flagg
President
Federal Flight Deck Officers Association (FFDOA)

email: mflagg@ffdoa.org

Website: www.ffdoa.org

VerDate Nov 24 2008 10:49 Sep 11, 2012 Jkt 067123 PO 00000 Frm 01326 Fmt 6601 Sfmt 6601 P:\DOCS\67123.TXT SAFFAIRS PsN: PAT

67123.944

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Joseph I. Lieberman

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

Question#:	1
Topic:	pre-check
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: A trusted traveler program could increase security by allowing TSA to focus its limited resources on the highest risk passengers. But it cannot compromise security and must ensure passengers that opt to enroll in TSA's Pre-Check Pilot are in fact trusted travelers..

For instance, a government approved identification document presented to TSA may be valid, but it may not belong to the passenger who is presenting it. How is TSA ensuring that the people considered trusted travelers are exactly who they say they are? Should these trusted travelers have to provide further confirmation to TSA that they are who they say they are, with a biometric identification?

Response: The Transportation Security Administration (TSA) currently validates passenger identification documents and boarding passes using Travel Document Checker procedures conducted by the Transportation Security Officers who are trained to detect fraudulent documents and are generally equipped with black lights, loops, and other fraud detection tools. In July 2011, TSA conducted lab testing of Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS) technology, which verifies passenger boarding passes and aids in the detection of fraudulent IDs that are presented to TSA by passengers during the security checkpoint screening process, as well as those IDs presented by airport and airline personnel to access sterile areas. In September 2011, TSA purchased a total of 30 CAT/BPSS systems from 3 different vendors for testing at select airports in early 2012.

TSA does not currently have plans to incorporate biometrics into checkpoint screening technologies. The physical screening of passengers and their baggage, additional random and unpredictable measures, and document validation provide strong protections against a security breach.

67123.945

Question#:	1
Topic:	pre-check
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Trusted Travelers' names are still checked against government watchlists through TSA's Secure Flight Program before every flight. Is TSA considering using additional data, even commercial data if a passenger will agree to it, to inform decisions regarding trusted travelers?

Response: TSA is currently piloting the use of additional data through passenger participation in other U.S. Government vetting programs and the use of additional passenger-provided data through its TSA Pre✓™ concept. As with any pilot initiative, TSA is testing the TSA Pre✓™ concept with a small passenger population at limited airports. Only those passengers who opt-in and are in this population have the opportunity to participate at this time. TSA will explore expanding the program to additional passengers, airports and airlines. Additional data sources, including commercial data, are not part of the current or near-term proof of concept model.

Question: What is the goal of the Pre-Check Pilot and how will TSA evaluate its success before opening the program to a larger segment of passengers or airports?

Response: The goal of the TSA Pre✓™ proof of concept is to demonstrate scalable capabilities to identify a low-risk population, apply prescreening parameters, encode a low-risk designator onto boarding passes, read the boarding passes, route the low-risk travelers to the appropriate screening lane, and apply expedited screening procedures to the low-risk passengers, while incorporating random and unpredictable screening measures. As of early October 2011, at the four proof of concept sites, TSA has successfully demonstrated all of these capabilities. Back-end data flows, such as how the airlines and U.S. Customs and Border Protection (CBP) operate with TSA's Secure Flight system, help to create low-risk passenger designations. Airport operational efficiency considerations, such as staffing models for peak travel times in a fully loaded checkpoint lane, are now well understood. Other practices have been identified, such as how airlines can communicate opt-in requirements to their frequent flyer population and how to effectively train airport staff on the TSA Pre✓™ procedures.

TSA is now applying criteria, including checkpoint throughput capacity and Global Entry participation, to identify other airports as candidates for TSA Pre✓™. Additional airlines are planning to participate, driving up the volume of known travelers eligible for expedited security procedures.

Question: Currently, a private company operating in two airports gathers information and verifies the identity of passengers who wish to pay to become trusted travelers, under TSA's Registered Traveler program. In exchange, these trusted travelers are able to avoid security lines. How will TSA leverage this program if it expands its risk-based screening programs, including Pre-Check?

Response: TSA is currently piloting the TSA Pre✓™ concept with a small passenger population at a limited number of airports. TSA plans to expand the concept to include additional passengers, airports, and airlines. TSA remains open to innovative ideas and solutions from the private sector and other sources.

67123.946

Question#:	2
Topic:	assessor pilot
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Assessor Pilot is another pilot program in which TSA is trying a new, more risk-based method of security. How will TSA demonstrate that this pilot is successful, and a wise use of resources given the high costs of personnel?

Response: The Transportation Security Administration (TSA) is working closely with the Department of Homeland Security Science and Technology Directorate (DHS S&T) to assist in validating the efficacy of the Assessor concepts. At each stage of the pilot, TSA will collect metrics to examine the effect of Assessor on security effectiveness, operational efficiency, and the passenger experience.

67123.947

Question#:	3
Topic:	mail
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Evaluating the risk and screening mail – which comprises a significant amount of cargo – is a particularly difficult endeavor. What will TSA do to address the impediments to assessing and screening mail?

Response: The Transportation Security Administration (TSA) and the United States Postal Service / United States Postal Inspection Service continue to assess vulnerabilities and develop security solutions for domestic aviation mail. This includes examination of technologies that could prove effective in screening for explosives, while considering current requirements to protect the privacy of the mail.

Mail transported inbound to the U.S. is handled as cargo. After the Yemen incident of October 2010, TSA added further requirements for mail screening in the Security Programs that identifies elevated risk categories, and appropriate enhanced screening procedures for those shipments transported on flights bound for the United States.

67123.948

Question#:	4
Topic:	investment
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Do you believe it would be useful, or that there is a need, for additional investment by the private sector in developing new aviation security technologies?

Response: The Transportation Security Administration (TSA) continues to work closely with the security technology industry to communicate requirements and necessary capabilities for security technologies. Since early 2010, TSA has issued an annual Broad Agency Announcement to collect innovative concepts from industry and to identify technologies already available in the marketplace. TSA has pursued several submissions for proof of concept demonstrations focused on insider threat analysis, behavior detection and explosives detection, and is currently reviewing numerous other proposals.

67123.949

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Carl Levin

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

Question#:	5
Topic:	travelers
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Eligible participants in TSA's Pre-Check pilot include certain select frequent flyers from Delta and American Airlines who opt in and members of Customs and Border Protections Trusted Traveler programs.

Eligible travelers that participate in Customs and Border Protection (CBP) known traveler programs have undergone background checks. However, frequent flyers have not undergone background checks. From a security standpoint, is the frequency that a person flies the correct criteria on which to base security risk as compared to someone with a security clearance or background check?

Response: Recent intelligence and past aviation security experiences indicate that the vast majority of passengers traveling domestically in the aviation system do not have the intent nor the means to bring catastrophic failure to an aircraft. The Transportation Security Administration (TSA) considered various intelligence and risk assessment factors, which for security reasons, will need to be provided in a classified setting, when determining the eligibility criteria for the pilot program and expedited screening. Opted-in, eligible TSA Pre✓™ travelers are still subject to the full range of watch list vetting, behavioral detection, selection for standard screening as determined by TSA, and other countermeasures.

Question: The U.S. Travel Association recommends expanding the program to including federal government employees or members of the armed forces with an active security clearance, and active federal law enforcement officials. How does TSA plan to expand Pre-Check to include other low-risk populations?

Response: TSA is exploring the feasibility, risks, and benefits of adding other identifiable low-risk populations to increase the volume of known travelers. For example, TSA is currently partnering with the Department of Defense (DoD) to test a military identification card-reading pilot for U.S. Armed Forces members traveling out of

67123.950

Question#:	5
Topic:	travelers
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Monterey Peninsula Airport. Members will be required to present their DoD identification to the TSA Travel Document Checker at the checkpoint where it will be scanned as part of the card-reading pilot. The pilot in Monterey is designed to test the technology and IT connectivity necessary to verify the status of U.S. service members; there will not be a change in physical screening. If successful, the card reading pilot could pave the way for members of the Armed Forces to be included in the TSA Pre✓™ expedited screening program.

TSA is exploring numerous options for expanding the low risk population to include individuals with security clearances. Once TSA has determined the initial feasibility and legal, privacy, and policy implications of incorporating a new population a proof of concept will follow, then operational evaluation, and then expansion based on findings from the evaluation.

Question: Passenger participation in Pre-Check is drawn from a number of existing CBP programs, all with differing criteria and costs. How are the different programs going to be combined and standardized if Pre-Check is expanded?

Response: TSA closely coordinates with U.S. Customs and Border Protection (CBP). Expansion of TSA Pre✓™ does not itself require combination or standardization of the CBP programs because the differences among the CBP programs do not affect how the TSA Secure Flight system receives data from CBP for TSA Pre✓™ purposes. U.S. citizens who are members of existing Trusted Traveler populations such as Global Entry, NEXUS and SENTRI are eligible for TSA Pre✓™. CBP has taken action to integrate its Trusted Traveler programs. Beginning in December 2010, Global Entry benefits were extended to NEXUS and SENTRI members. In July 2011, CBP implemented a single application on its Global Online Enrollment System (GOES) website. Program applicants are now able to submit one application and apply for multiple programs. In addition, CBP began issuing Global Entry cards. The Global Entry card is radio frequency identification (RFID) enabled and allows Global Entry members to use the dedicated commuter lanes (NEXUS or SENTRI) at the land borders when entering the U.S.

Question: If Pre-Check eventually means a large segment of the flying public can have expedited security screening will that ultimately mean less screening equipment will be needed? If that is the case, does TSA have a model for efficiencies to be gained?

Response: TSA is in the early pilot phase with TSA Pre✓™. Data is being collected and will be analyzed to inform expansion and possible efficiencies moving forward.

67123.951

Question#:	6
Topic:	risk-based
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: As part of TSA's risk-based intelligence-driven approach, TSA is piloting an expanded behavior detection program in Boston and Detroit expanding on existing Screening of Passengers by Observation Techniques. In the behavior detection pilot, specialized behavioral analysis techniques will be used to determine if a traveler should be referred for additional screening at the checkpoint.

Do the officers ask every passenger questions and is there an approved list of questions?

Response: Under the current concept of operation, all passengers are asked a few questions after they have their ID and boarding pass checked at the travel document checker podium position. Questions are outlined in the Assessor training course and standard operator procedures for the Transportation Security Administration (TSA) employees who have received assessor training to use as appropriate.

Question: What indicators are the Behavior Detection Officers (BDO) looking for? Are they trained to look for a nervous tick or a hesitation? How do they factor in people who are nervous about flying?

Response: The TSA employees who have received assessor training are trained to look for behavioral indicators that may be indicative of a threat to transportation security. For security reasons, specific indicators will need to be provided in a classified setting. Even though someone may be "nervous," this individual indicator is not enough for the assessor to refer for additional screening. It is the totality of the encounter and all relevant information that forms a decision to refer someone for additional screening.

Question: What criteria are used to determine if a passenger warrants additional screening? Is it based solely on how a person answers the questions? Is there any consideration for ethnic origin or dress? There have been reports of people being asked to leave a plane based on their appearance. Will appearance be a factor in this screening process?

Response: Screening of persons and property is conducted in accordance with all applicable anti-discrimination laws, regulations, Executive Orders, policies and directives and without regard to a person's race, color, national origin, gender, disability, religion, parental status , or sexual orientation. The TSA employees who have received assessor training are trained to look for behavioral indicators that may be indicative of a threat to transportation security. For security reasons, specific indicators will need to be provided in a classified setting. It is the totality of the encounter and all relevant information that forms a decision to refer someone for additional screening.

67123.952

Question#:	6
Topic:	risk-based
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Is there any weight given to where the passenger is from or where he or she is going, such as the Middle East that would increase their chances of getting additional screening?

Response: Screening of persons and property is conducted in accordance with all applicable anti-discrimination laws, regulations, Executive Orders, policies and directives and without regard to a person's race, color, national origin, gender, disability, religion, parental status, or sexual orientation. TSA employees who have received assessor training are trained to look for behavioral indicators that may be indicative of a threat to transportation security. For security reasons, specific indicators will need to be provided in a classified setting. It is the totality of the encounter and all relevant information that forms a decision to refer someone for additional screening.

67123.953

Question#:	7
Topic:	human remains
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: It was brought to my attention by a Michigan funeral director that human remains are exempt from the 100 percent screening requirement for air cargo transported on passenger aircraft. I was further informed that a voluntary certification is available through TSA's Certified Cargo Screening Program but that most funeral homes and mortuaries may not seek this certification because it is not required.

Why are human remains being excluded from the cargo inspection process?

Does this exclusion pose any risks?

Response: The Transportation Security Administration (TSA) requires that for shipments originating in the U.S., all human remains must be from a known shipper and are subject to alternative security measures contained in the air carrier security programs. TSA is currently working with the carriers and the human remains industry to update screening requirements and to incorporate the use of a variety of screening technologies to increase the level of screening while still maintaining the sanctity of human remains shipments. The Known Shipper database provides a systematic approach to assess risk and determine the legitimacy of shippers. Passenger Air Carriers and Indirect Air Carriers must comply with a broad range of specific security requirements to qualify their clients as Known Shippers.

67123.954

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Mary L. Landrieu

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

Question#:	8
Topic:	body scans
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: Body scans and pat-downs were implemented by TSA after a terrorist smuggled a non-metallic bomb aboard Northwest flight 253 in an attempt to destroy it on its way from Amsterdam to Detroit on Christmas Day in 2009. TSA has adopted new technology to make body scans more anonymous, but pat-downs remain intrusive and particularly controversial when small children, the elderly, and the disabled are subjected to a search. TSA revised screening procedures for children aged 12 and under in September, it issued 6 informational Job Aids in FY11 focused on screening for special needs populations, and it has re-designed training for screening Persons with Disabilities and Medical Conditions to address disabilities, mobility devices, medical appliances, and prosthetics. Why are pat-downs included in the screening process at all, and what will it take to completely and permanently replace them with a less intrusive method?

Response: Before the attempted terrorist attack in December 2009, the Walk Through Metal Detector (WTMD), hand-held metal detector (HHMD), and pat-down of areas that caused metallic alarms were used to screen individuals at U.S. airports. Individuals unable to undergo metal detection screening received a pat-down. The December 25, 2009 incident aboard Northwest flight 253 demonstrated that the metal detection and pat-down procedures in place in U.S. airports were not adequate to detect non-metallic threats, including improvised explosives devices, concealed on an individual such as the device Umar Farouk Abdulmutallab attempted to detonate.

Advanced Imaging Technology (AIT) is the only technology in place that is able to detect both metallic and non-metallic threats concealed under clothing on an individual. For those individuals who either cannot or choose not to undergo AIT, a pat-down, followed by explosives trace detection, is a comparable level of screening. The pat-down is also the most effective method for resolving an anomaly identified during AIT screening. Elimination of the pat-down would lessen the overall effectiveness of screening and make it difficult to resolve anomalies detected by the AIT. It would also remove an alternative for persons who cannot or chooses not to undergo AIT screening. Without the availability of the pat down and explosive trace detection, an adversary could circumvent the AIT and conceal a non-metallic threat on his or her person that would not be caught with an alternative technology, such as the WTMD. The pat-down plus explosives trace detection better mitigates this vulnerability.

The Transportation Security Administration (TSA) will continue to evaluate new technologies and screening procedures to provide the most effective security in the most efficient manner.

67123.955

Question#:	9
Topic:	collective bargaining
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: The House passed a provision as part of the FY 2012 Homeland Security Appropriations bill that would prohibit TSA from implementing collective bargaining for transportation security officers. The Senate rejected a similar amendment during debate of the Federal Aviation Administration re-authorization bill earlier this year. In February, you made the decision to grant transportation security officers limited bargaining rights and you prohibited bargaining on security policies and procedures. You testified that, "TSA will not bargain on security." This was a smart decision and as Chair of the Senate Homeland Security Appropriations Subcommittee, I will be fighting against the House prohibition because even with the limited nature of TSA's collective bargaining decision, it will boost employee morale and provide them with a voice in the workplace.

Do you believe that this collective bargaining agreement will improve the performance of the TSA workforce and therefore improve security?

Response: The Transportation Security Administration (TSA) believes that a union can play a constructive role by helping to identify and develop solutions for certain systemic challenges facing the TSA workforce. The matters that are subject to negotiation with the union are specified in a February 4, 2011 Determination issued by the TSA Administrator, and exclude security-related policies/procedures. For the specified matters subject to negotiation, collective bargaining will provide a structure for front-line employees to have a strong voice to raise workplace issues and to promote consistency in management practices across the 450 airports served by TSA.

Question: How are Transportation Security Officers trained to handle children and Persons with Disabilities and Medical Conditions?

Response: TSA employs a variety of training methods and adult learning techniques, which include instructor-led classroom lectures and scenario based reviews; web-based interactive sessions which are decision driven; and training sessions which include practical application /demonstration, hands-on labs, and role playing. In addition to learning how to appropriately screen children and passengers with disabilities, specific screening options that Transportation Security Officers (TSOs) are trained to employ when screening children and passengers with disabilities include:

- Minors and passengers with disabilities should not be separated from their traveling companions or family members. Companions or family members are informed that they may have to be re-screened after assisting their child or family member with a disability through the screening process.

67123.956

Question#:	9
Topic:	collective bargaining
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

- Individuals may request private screening and have a witness of their choosing accompany them during the private screening.
- Persons with disabilities, caregivers, and/or family members may request to be moved to the front of the screening line or TSA can offer this option to those individuals.
- Medical information should be acknowledged and reviewed by a TSO (if offered) to better understand a person's disability in order to facilitate the screening process. Medical documentation does not exempt passengers from screening.
- TSOs are trained to respect a passenger's privacy by not discussing the disability in front of other passengers. Discussion with other TSA employees about the individual's disability is limited to only those who have a "need to know" in order to complete the screening process.
- Persons with disabilities are treated with sensitivity when a TSO is informed that an individual has just undergone a traumatic operation/procedure or has a medical condition which may be causing emotional distress and/or pain.
- Passengers with disabilities are not required to do things that will cause them pain or are beyond their level of ability. For example, passengers can remain seated while being screened or can be screened without taking their shoes off when necessary.
- Medically necessary liquids and nutrition for infants, such as breast milk and formula, are permitted in excess of TSA's 3-1-1 rules after they have been appropriately screened.

Question: What changes have been made along the way?

Response: The Transportation Security Administration (TSA) has made the following changes to ensure the proper screening of children and persons with disabilities and medical conditions:

- New Hire Training Program lessons were redesigned to ensure that information about screening of persons with disabilities and medical conditions is included during all phases of the training, rather than as a separate training module.
- Job aids and recurrent training courses were and are continually updated to enhance the training associated with the screening of persons with disabilities and medical conditions.
- Recurrent training products were revised to include additional screening procedures of persons with disabilities and medical conditions.

67123.957

Question#:	9
Topic:	collective bargaining
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

- A tailored training process was established to reinforce screening procedures at the ten airports where Cast Prosthetic Imager (CPI) equipment is deployed.
- A course was launched that facilitates better communication between Transportation Security Officers (TSOs) and all individuals undergoing the screening process to help prevent potentially confusing, confrontational, or unpleasant encounters.
- The instructor program was reviewed and revised so that it better supports the on-the-job portion of persons with disabilities and medical conditions training.
- A new series of Supervisory and Lead TSO recurrent training was launched that presents scenarios, including persons with disabilities and medical conditions, and allows them to make decisions at critical junctures and see the consequences of their decisions.

67123.958

Question#:	10
Topic:	aviation security
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: The Senate version of the FY12 Homeland Security Appropriations bill includes the following important provisions related to aviation security:

a. $10 million for TSA to implement the Trusted Traveler Program, which was not included in the House bill;
b. A requirement for TSA to improve its response to passenger complaints along with a GAO review of existing procedures, which was not included in the House bill;
c. A requirement that TSA screen passengers and crew in a manner consistent with privacy laws, which was also included in the House bill;
d. Report language directing TSA to improve training to address passengers with physical or mental disabilities like autism, which was not included in the House bill;
e. $100 million to purchase, install, and operate 275 additional Advance Imaging Technology (AIT) units in addition to the 1,000 machines already operating around the country in 2,100 airport lanes, which is not included in the House bill;
f. $11 million above the FY11 level to add 175 new Behavior Detection Officers, which was not included in the House bill;
g. A 5-year strategic investment plan for passenger screening technologies, which was not included in the House bill;
h. A requirement that the TSA's FY13 budget request document resource allocation on the basis of risk, which was not included in the House bill; and
i. FY12 expenditure plan for explosives detection systems, checkpoint support technologies, and air cargo security; which was also included in the House bill.

Please describe the impact that these House-proposed cuts would have on TSA's efforts to improve security and convenience at passenger screening checkpoints, in particular with regard to deployment of AIT machines and Behavior Detection Officers.

Response: If provisions proposed in the House bill are not modified in the Conference bill, the Transportation Security Administration (TSA) would face major impacts in several key aviation security programs. The following impacts, by item, include:

a. Trusted Traveler Program. Without the $10M, TSA will be unable to develop a systems architecture or procure hardware and software to handle expanded processing requirements to support proof of concepts and incremental capabilities to expand the known traveler populations.

b. No funding impact.

c. No funding impact.

67123.959

Question#:	10
Topic:	aviation security
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

d. No funding impact.

e. Advanced Imaging Technology (AIT). AIT units screen passengers for concealed metallic and non-metallic weapons, explosives, and other prohibited items, and is the most effective passenger screening technology currently available. TSA has found a high degree of passenger acceptance for screening by AIT. Funding for an additional 275 AIT units would increase the number of passengers screened by this technology from 60 percent to 80 percent. Absent support for additional AIT units, TSA will continue to employ alternative screening methods including the use of metal detectors which do not detect non-metallic threats.

f. Behavior Detection Officers. TSA's Screening of Passengers by Observation Techniques (SPOT) program is a behavior and analysis security program in which personnel are trained to identify anomalous behaviors that deviate from an established environmental baseline. SPOT personnel, known as Behavioral Detection Officers (BDOs), observe the security checkpoint to identify passengers displaying potentially high-risk behaviors which may be indicative of a threat to transportation security. In FY 2010, SPOT referred 50,172 passengers for additional screening resulting in 3,569 law enforcement officer calls and yielding 314 arrests.

The current SPOT program is comprised of approximately 3,000 BDOs at 161 airports. BDOs serve as an additional layer of security in airports by providing a non-intrusive means of identifying individuals who may pose a risk of terrorism. The additional 175 Full-Time Equivalents (FTE) would comprise 87 additional behavior detection teams. These additional teams would allow more thorough coverage at some of the largest and highest risk locations as well as expand the program to some smaller airports which do not currently have this layer of security. Failure to gain approval for the additional FTE would preclude the additional coverage and expansion into smaller airports.

g. No funding impact.

h. No funding impact.

i. No funding impact.

67123.960

Question#:	11
Topic:	crewmembers
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Mary L. Landrieu
Committee:	HOMELAND SECURITY (SENATE)

Question: The Known Crewmember initiative allows crewmembers to forego screening if they show two forms of verifiable identification. Pilots are eligible to enroll, but flight attendants are not.

Why were flight attendants excluded from the Known Crewmember pilot program?

Response: The Transportation Security Administration (TSA) prioritized applying the Known Crewmember concept to the crewmembers who are most capable of causing harm to an aircraft and passengers since they are in control of the aircraft. Physical screening of pilots is not as effective since they have the skill and opportunity to cause harm and would not need prohibited items in order to do so. The Known Crewmember initiative works to tie airline employee databases together in a seamless way and enable TSA security officers to positively verify identity and employment status of crewmembers.

The seven airports with Known Crewmember will complete their pilot activities in late January 2012. At that time, TSA will have additional data to assess the effectiveness of the concept and determine whether it should be expanded.

Known Crewmember is jointly sponsored by the Airline Pilots Association (ALPA) and the Air Transport Association (ATA).

67123.961

Post-Hearing Questions for the Record
Submitted to the Honorable John S. Pistole
From Senator Susan M. Collins

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

Question#:	12
Topic:	SPP
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Administrator Pistole, earlier this year you decided not to approve the expansion of the Screening Partnership Program (SPP), which allows private screeners to operate at 16 airports. As you know, this was a major topic in the Senate earlier this year during consideration of the FAA reauthorization bill. Can you please explain the reason for your decision to not allow more airports to participate in this program?

Response: Shortly after Administrator Pistole was confirmed as Transportation Security Administration (TSA) Administrator, he directed a full review of TSA policies and programs to help the agency evolve into a more agile, high-performing organization that can detect and respond to the security threats of today and the future. The Screening Partnership Program (SPP) was one program that was reviewed. At the time, it was determined there was no clear and substantial advantage to expanding the SPP program, though TSA remained committed to maintaining contractor screening where it then existed. TSA is open to approving new SPP applications where such a clear and substantial benefit could be realized.

67123.962

Question#:	13
Topic:	FirstLine
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Recently, FirstLine, a private sector screening partner at the Kansas City Airport, won a U.S. Court of Appeals decision regarding TSA's award of a screening contract to a lower-cost, but according to the Court, technically inferior competitor. The Court agreed with the plaintiff that TSA's award decision was "irrational and contrary to the RFP." In addition, the Court took issue with TSA's conclusion "that the higher technical merit offered by FirstLine's proposal did not outweigh [the successful bidder's] price advantage."

It is obvious that agencies must strongly justify decisions to pay a price premium when there is clear evidence that a higher priced proposal will provide the best value to the government, it is equally important that agencies provide strong justification when deciding not to award a contract to the contractor with the strongest proposal. To do otherwise when using a "best value" source selection approach is simply not fair to contractors and leaves the impression that the agency is not serious about seeking the best value for the American taxpayer.

What is TSA doing to ensure that it improves upon its source selection processes?

Response: Regarding the two issues (of eight raised) on which the Court ruled in favor of FirstLine, the Transportation Security Administration (TSA) has identified some lessons learned which will be applied not only to future SPP source selections, but to source selections across TSA. These lessons are:

- TSA will ensure that every Source Selection Evaluation Board (SSEB) understands that as part of a best-value trade-off analysis, comparisons must go beyond summary technical adjectival ratings and consider in detail the strengths, weaknesses, benefits, and disadvantages of the proposals. TSA will also ensure that its SSEBs understand that such comparisons need to be well-documented.
- TSA will ensure that each Source Selection Authority (SSA) understands that their award decision should not just be a "sign-off" of the SSEB's evaluation, and that the SSA must instead perform and document an independent assessment and evaluation of the competing proposals.

Question: How is TSA addressing the many shortfalls identified in the Court of Federal Claims recent decision?

Response: See the response in (a) above. More specifically, as a result of the Court's decision TSA intends to issue a completely new solicitation for screening services at Kansas City International Airport. This solicitation will correct the price evaluation scheme errors and other shortfalls identified by the Court, and will also reflect the numerous changes and updates that have occurred since the original solicitation was released.

67123.963

Question#:	14
Topic:	USTA
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Secretary Ridge and the US Travel Association released a report in March titled "A Better Way: Building a World Class System for Aviation Security." In that report, USTA stated that TSA should reinstitute the Aviation Security Advisory Committee, among other things.

Can you describe how this would benefit the aviation security environment?

Response: The Aviation Security Advisory Committee (ASAC) enhances the Transportation Security Administration's (TSA) security posture through consultation with key partners concerning potential risks to infrastructure, passengers, and cargo. In addition, the committee gathers input from stakeholders on the effectiveness of security procedures and develops recommendations for improvements to aviation security methods. ASAC was effectively reinstituted on October 27, 2011, and TSA has notified the organizations and individuals that have been appointed to serve.

67123.964

Question#:	15
Topic:	process
Hearing:	Ten Years After 9/11: The Next Wave in Aviation Security
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: The US Travel Association also recommended that TSA develop and utilize a risk management process to better allocate its resources. As we know, in our current financial environment all cost savings should be looked at, especially those that can enhance security.

Can you please describe what, if anything, you are doing to implement this recommendation beyond the current RBS initiative?

Response: The Transportation Security Administration (TSA) continually looks for ways to enhance its layered security approach through new, state of the art technologies, expanded use of existing and proven technologies, better passenger identification techniques, and other developments that will strengthen our existing capabilities. TSA is undertaking efforts to focus its resources and improve the passenger experience at security checkpoints by applying new risk-based, intelligent-driven screening procedures and enhancing its use of technology. Beyond the Risk Based Screening (RBS) initiative, TSA makes resource allocation and technology decisions informed by considerations of risk, including threat, vulnerability, and consequence analysis. TSA has conducted comprehensive, strategic-level risk assessments in the transportation modes. These assessments combine assessments of threat, vulnerability, and consequence to produce comparative analyses of risk within each mode and a comparative risk analysis for the transportation sector. In addition, TSA develops technology and makes resource recommendations in accordance with a strategic implementation plan to close known security gaps. TSA bases investments on analyses of alternatives and test and evaluation of technologies in a simulated environment. TSA engages in pilot programs to test new approaches before committing limited resources to enable the collection of data and assess the results before moving forward. Through these practices, TSA has been able to generate cost savings and reinvest those savings in efforts to enhance security.

67123.965

Post-Hearing Questions for the Record
Submitted to Roger J. Dow
From Senator Joseph I. Lieberman

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1.) A trusted traveler program could increase security by allowing TSA to focus its limited resources on the highest risk passengers. But it cannot compromise security and must ensure passengers that opt to enroll in TSA's Pre-Check Pilot are in fact trusted travelers.

A government approved identification document presented to TSA may be valid, but it may not belong to the passenger who is presenting it. Should these trusted travelers have to provide further confirmation to TSA that they are who they say they are, with a biometric identification?

Chairman Lieberman, in the U.S. Travel report on aviation security, our panel of experts recommended that trusted travelers be required to use some form of biometric identification to verify their identity before going through expedited screening. The panel recommended biometric identification because currently it is one of the most secure forms of identification and security is critical to the long-term success of PreCheck. As enrolment in PreCheck grows, the TSA should consider requiring trusted travelers to use biometric identification.

If the program is voluntary, should TSA consider using additional data, even commercial data if a passenger will agree to it, to inform decisions regarding trusted travelers?

Chairman Lieberman, the U.S. Travel blue ribbon panel on aviation security also recommended that TSA use commercial data as one element of a risk assessment conducted on trusted travelers. As enrolment in PreCheck grows, the TSA should seek to use voluntarily provided commercial data as one element of a risk assessment on trusted travelers.

2.) You testified in support of TSA's initial steps to pilot some risk-screening programs, which are important but modest steps forward designed to test new ideas. How would you suggest DHS and TSA scale up or build upon these initial risk-based screening programs?

67123.966

Chairman Lieberman, the TSA should scale up its trusted traveler program by leveraging the private sector, airports, and populations already verified as low risk by the federal government. The TSA should leverage the private sector by partnering with approved Registered Traveler providers who have an incentive to market and grow enrolment in PreCheck. The TSA should also form a partnership with the airports and organizations like the American Association of Airport Executives (AAAE) that already assist the Department of Homeland Security in performing risk assessments on airport workers. The AAAE could help to expand enrolment in PreCheck by performing similar risk assessments for trusted travelers on behalf of TSA. Lastly, the TSA should seek to leverage existing populations of trusted individuals, such as federal employees with Top Secret clearances, Transportation Worker Identification Card (TWIC) holders, and members of the U.S. armed forces.

3.) Do you believe that TSA, airlines, and local airport and law enforcement authorities should reexamine their relationships and authorities at and near the checkpoint? How could this improve efficiency or mitigate confusion, or why might we need to continue to differentiate between TSA and local authority at the checkpoint?

Chairman Lieberman, the U.S. Travel Association believes that the TSA, airlines, and airports should reexamine their relationship as it relates to control of the checkpoint. When travelers arrive at the airport, they do not distinguish between queuing lines, which are controlled by the airports or airlines, and the security screening area, which is controlled by TSA. Travelers see the checkpoint as singely controlled by TSA. As enrolment in PreCheck is expanded, control of the queuing lanes will become more important and TSA will need the flexibility to determine where queuing lines should be placed to have the greatest benefit on security and efficiency. As such, the TSA, airlines, and airports should reexamine their relationship at the checkpoint to give TSA more control over where trusted traveler lanes are placed and the layout of both the queuing lines and the screening area.

67123.967

Post-Hearing Questions for the Record
Submitted to Roger J. Dow
From Senator Thomas R. Carper

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1. In your testimony, you discussed how the current "one-size-fits all" screening process at our airports does not meet the needs of the traveling public and that we should look at moving to a system that detects dangerous people instead of only dangers things. As you know, this Committee has continually challenged government officials to work smarter with federal dollars and to find efficiencies in our government programs without compromising security. To this end, I understand the Transportation Security Administration (TSA) has developed a pilot to help expedite the flow trusted travelers, but there is still much room for growth. Can you discuss the challenges TSA may face as it looks to expand the pilot and how industry can help find solutions to these issues?

Senator Carper, as the TSA seeks to expand PreCheck it will face a significant challenge in enrolling a sufficient number of passengers to make the program efficient and reduce wait times for all travelers. The TSA must have a large population of PreCheck enrollees to ensure consistent throughput in trusted traveler lanes, a decrease in throughput in regular queuing lanes, and to allow for an efficient use of resources. Using only the current enrollment methods for PreCheck – namely frequent flyer history and U.S. Customs and Border Protection (CBP) trusted traveler programs – we believe TSA will be unable to reach such a critical mass. For example, when travelers join PreCheck through a sponsoring airline those passengers can only utilize the program when flying with that particular carrier (e.g. a Delta PreCheck enrollee is not an American Airlines PreCheck enrollee). This limits participation in PreCheck and lessens the program's value for flyers.

The travel industry can assist TSA in growing PreCheck and reaching a critical mass of participants by marketing CBP trusted traveler programs. For example, American Express currently offers to pay the Global Entry enrollment fee for its customers as a way to expand participation in Global Entry and provide a benefit to its cardholders. American Express and other travel businesses could boost their marketing efforts for CBP's trusted traveler programs as a way to expand PreCheck. Moreover, if TSA were to allow travelers to join PreCheck using Registered Traveler providers, the travel industry could also market that method of enrollment to its customers.

67123.968

Post-Hearing Questions for the Record
Submitted to Roger J. Dow
From Senator Mary L. Landrieu

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1. The U.S. Travel Association recommended that base airfare include the cost of one checked bag in its bipartisan report, "A Better Way: Building a World Class System for Aviation Security." When Secretary Napolitano testified before this committee earlier in the year about the President's budget request for the Department of Homeland Security in FY12, she indicated that TSA incurred additional costs of $259 million last year to screen increased volumes of carry-on baggage that has emerged since airlines began charging for the first checked bag. As Chairman of the Homeland Security Appropriations Subcommittee, I am upset that airline fees are increasing TSA's operating costs at a time when the Department is already facing severe budget cuts. Meanwhile, the fees are generating billions of dollars in annual revenues for the airlines, and yet they are not required to compensate TSA for these increased costs, and their per-ticket security tax has not increased at all since TSA was established 10 years ago. In addition to the budgetary strain that checked baggage fees produce for TSA's operating costs, what are the impacts of these fees on passenger volume in general and the travel and tourism industry overall?

Senator Landrieu, the recent trend of most airlines charging separate fees for every checked bag has resulted in airline passengers "carrying on" substantially more baggage per person. The increased volume of carryon baggage is causing significant checkpoint congestion, leading to longer wait times, and becoming a top frustration of travelers. According to the TSA, transportation security officers are screening almost a million more carry-on bags per day since the widespread implementation of checked bag fees. This is making it harder for TSA to identify dangerous items in carry-on bags, leading to longer screening times for each bag, and slowing down the security checkpoint.

In addition, according to a recent survey conducted by U.S Travel, an overwhelming majority of passengers (74 percent) said their top frustration with flying was passengers who brought too many carry-on bags through the security checkpoint.

What we know from repeated research is that inefficiencies in the checkpoint process are causing Americans to avoid flying. For example, a 2010 survey conducted by Consensus Research found that American travelers would take an additional two to three flights per year if the hassles in security screening were eliminated. These additional flights would add nearly $85 billion in consumer spending and support 900,000 American jobs.

67123.969

2. The U.S. Travel Association has recommended the establishment of a Trusted Traveler Program, and TSA's Pre-Check pilot program launched last month represents this administration's attempt to create one. You make the point in your testimony that the program must significantly improve traveler convenience in order to incentivize large-scale enrollment. After all, program participants are required to undergo a background check and register their biometric data with TSA in order to qualify, so it is important to consider what they stand to gain in return for their troubles. Do you feel that TSA's Pre-Check program provides a sufficient degree of incentives? What changes would you suggest to further incentivize enrollment?

Senator Landrieu, the TSA can do three things to provide a greater value in the PreCheck program. First, the TSA should allow PreCheck enrollees to use the program when flying on any airline that is participating in the program. Under the current system, when travelers join PreCheck through a sponsoring airline those passengers can only utilize the program when flying with that particular carrier (e.g. a Delta PreCheck enrollee is not an American Airlines PreCheck enrollee). This limits participation in PreCheck and lessens the program's value for flyers. By allowing PreCheck enrollees to use the program when flying with any participating carrier, TSA can increase the value of the program.

Second, as the PreCheck program grows, the TSA should provide dedicated queuing lanes for all PreCheck enrollees. Under the current program, some airports do not have separate queuing lanes for PreCheck passengers. This means that PreCheck participants must wait in the standard queuing lines until they reach the Travel Document Checker (TDC), at which point they are separated into a different screening line. By making PreCheck participants wait in the standard screening line, TSA is providing little efficiency benefit for these enrollees. TSA can provide a greater value for PreCheck passengers by providing separate queuing lanes for program participants wherever airport pace is available.

Third, Administrator Pistole stated on a number of occasions that PreCheck enrollees will be randomly selected for additional screening, instead of the expedited screening. This is a sensible and prudent security measure. However, if PreCheck enrollees are selected for additional screening during a high percentage of their trips, they will still be forced to arrive at the airport well in advance of their flight in order to plan for the likelihood of increased wait times. In that scenario, PreCheck passengers would likely see the program as providing little efficiency benefit. Therefore, TSA should seek to use enrollment criteria that provides the best indication of risk and allows PreCheck enrollees with predictable wait times in the screening process - even if the actual screening procedures vary to provide a needed degree of randomness.

Post-Hearing Questions for the Record
Submitted to Kenneth J. Dunlap
From Senator Joseph I. Lieberman

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1.) A trusted traveler program could increase security by allowing TSA to focus its limited resources on the highest risk passengers. But it cannot compromise security and must ensure passengers that opt to enroll in TSA's Pre-Check Pilot are in fact trusted travelers.

A government approved identification document presented to TSA may be valid, but it may not belong to the passenger who is presenting it. Should these trusted travelers have to provide further confirmation to TSA that they are who they say they are, with a biometric identification?

If the program is voluntary, should TSA consider using additional data, even commercial data if a passenger will agree to it, to inform decisions regarding trusted travelers?

IATA applauds TSA's commitment to innovation and their progress to date on the Pre√™ system. IATA believes that Known Traveler programs serve as a cornerstone of next generation passenger screening. We encourage TSA to expand the pilot to other airports so that more passengers benefit from expedited screening measures. As the Chairman is aware, IATA believes that biometric identification plays a key role in the next generation passenger screening checkpoint. We are currently studying ways in which this type of identity verification can be best used at the checkpoint to provide an additional layer of security. Our activity to date suggests that if biometric identity verification is used then it would be most appropriate to reduce any redundancy in the screening process that results from its incorporation.

With regard to the use of additional commercial data being used for kown traveler programs, we do not believe that this is necessary.

2.) You testified in support of TSA's initial steps to pilot some risk-screening programs, which are important but modest steps forward designed to test new ideas. How would you suggest DHS and TSA scale up or build upon these initial risk-based screening programs?

67123.971

In order to scale up or build upon existing initiatives there needs to be strong legislative and regulatory support. The best security programs are flexible and not prescriptive. This would argue that 100% legislative mandates that prescribe exact procedures or screening equipment to be employed may not be effective in promoting risk-based programs. Next, we believe that these screening programs would benefit from revised regulatory frameworks that are outcome focused and build on Security Management Systems. They in effect prescribe the desired outcome and not the path to the outcome as is currently done.

We would like to highlight for the Committee the UK's Better Regulation for Aviation Security initiative. This is a proposal for an outcome-focused, risk-based approach to security regulation which builds on the similar approach used for aviation safety. IATA believes that such a regulatory structure may be of interest to DHS and TSA as they pursue future plans.

3.) Do you believe that TSA, airlines, and local airport and law enforcement authorities should reexamine their relationships and authorities at and near the checkpoint? How could this improve efficiency or mitigate confusion, or why might we need to continue to differentiate between TSA and local authority at the checkpoint?

IATA believes that lines of communication between airlines and federal and local authorities should promote an open dialogue on critical security measures. Maintaining such a collaborative environment will improve efficiency and mitigate confusion that may arise at the security checkpoints. We believe there is always room to improve any relationship, but these do not rise to the level of national issues that require national solutions. We believe these can resolved at the local level.

4.) Do you believe that TSA could expand its pilot to include international flights or international passengers? Are other countries experimenting with similar trusted traveler programs and if so, what do you see as the lessons learned that TSA should keep in mind?

IATA would support the expansion of the current pilot to include international flights and their passengers. Currently, we are aware of 25 Known Traveler programs in use throughout the world. At the macro level there are similarities in the data requirements for membership. There is precedent within the US for recognition of compatible known traveler programs as demonstrated by CBP's FLUX program with the Dutch Privium known traveler program. We believe that for the pilot TSA could find compatible programs for recognition under Pre√™.

Post-Hearing Questions for the Record
Submitted to Kenneth J. Dunlap
From Senator Thomas R. Carper

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1. In your testimony, you discussed how the current "one-size-fits all" screening process at our airports does not meet the needs of the traveling public and that we should look at moving to a system that detects dangerous people instead of only dangers things. As you know, this Committee has continually challenged government officials to work smarter with federal dollars and to find efficiencies in our government programs without compromising security. To this end, I understand the Transportation Security Administration (TSA) has developed a pilot to help expedite the flow trusted travelers, but there is still much room for growth. Can you discuss the challenges TSA may face as it looks to expand the pilot and how industry can help find solutions to these issues?

IATA applauds TSA's commitment to innovation and their progress to date on the PreV™ system. IATA believes that Known Traveler programs serve as a cornerstone of next generation passenger screening. They fulfill a fundamental principle of the Checkpoint of the Future: passengers should be screened at the airport with devices and processes commensurate with what is known about them.

We believe that TSA may face a number of challenges in expanding the PreV™ pilot:

- Identifying additional categories of travelers eligible for PreV™ and establishing quick and convenient enrolment procedures for the higher volume
- Defining and quantifying additional data that may be needed for passenger risk analysis
- Adding additional airports to the pilot
- Making physical changes to checkpoint queuing areas to accommodate greater numbers of enrollees
- Maintaining or creating additional value propositions that incentivize travelers to enroll
- Identifying the role of biometric validation as part of any future expansion plans
- Expanding the risk based security paradigm across additional areas of TSA responsibility

IATA Member Airlines have a strong history of supporting government initiatives to speed passenger travel while enhancing security. Our airlines have supported programs such as Global Entry, INSPASS and NEXUS Air. We are 100% supportive and enthusiastic of PreV™.

67123.973

We would expect that additional new airlines will volunteer to participate in the pilot, perform the necessary automation upgrades, and devote dedicated project management teams to successfully complete the tasks to support PreV™ roll out. In addition, airlines can be expected to contact passengers eligible for the pilot through direct mail, email, and web-centric messaging campaigns. Member airlines have also worked in collaboration with TSA to fashion media campaigns to publicize the pilot.

2. I was intrigued by your discussion and images of the "checkpoint of the future," which would require: risk-based screening; the use of advanced screening technology; and separate lanes for different types of travelers. This type of checkpoint could improve security, as well as save travelers countless hours and ultimately help our local economies. While the concept seems simple, it may also require significant changes that might be difficult to implement in this fiscal environment. What would the "checkpoint of the future" cost and are there programs and technologies currently in place that can be seamlessly integrated into your vision?

Determining associated costs and the business case for a new passenger screening system are core objectives of the IATA Checkpoint of the Future program. With our research just beginning, it is too early to specify an exact cost breakdown. However, we can make several high-level observations:

Because the first phase of IATA's Checkpoint of the Future envisions repurposing existing checkpoints and their technologies, we do not anticipate large new capital investments. The near term intermediate checkpoint that we are pursuing and showed the Committee uses many of the same components and processes that are in use in today's airports. Expenses that we are aware of include the development of a known traveller program, physical rearrangement of a standard checkpoint into a 3 lane system, wiring to receive new data, and, in one proposal, deployment of a small aperture CTX explosive screening machine. There will also be costs associated with deployment of behavior detection officers and biometric identification systems.

To put some costs in perspective, TSA has already deployed a known traveller system called PreV™ , behavior analysis officers are already in some airports, and we believe that an intermediate checkpoint reconfiguration can be done in stages to manage costs. We believe that such a checkpoint could be functional within one year and airport ready with all regulatory approvals by the end of 2013.

In the longer term, we are pursuing "tunnels of technology" for deployment in 7-10 years. This will be built on the lessons learned from the intermediate checkpoint reconfiguration and will require some technologies that exist only in a laboratory related to standoff explosive detection. IATA appreciates that we are pushing the limits of technology in this vision, but our initial research shows that this is possible in the time frame of the next decade. We believe that given sufficient investment incentives, equipment manufacturers can mature the needed technologies. IATA will develop the business model for this screening experience as the lessons learned from the intermediate checkpoint become available.

Post-Hearing Questions for the Record
Submitted to Kenneth J. Dunlap
From Senator Mary L. Landrieu

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1. The International Air Transport Association has described the "checkpoint of tomorrow" as a system comprised of three screening lanes for three categories of travelers, who would be classified in advance as either Known Travelers (KT), Normal Screening (NS), or Enhanced Security (ES), depending on the level of threat they present based on advance analysis of their biographical information and travel documents. Such a system would also employ behavior detection analysis at the checkpoint itself. The U.S. borrowed the concept of behavior detection from the Israelis, and a prototype airport terminal was recently unveiled in Singapore. Are there aviation checkpoints or screening systems that you have observed elsewhere in the world that homeland security officials in the United States should examine in order to identify desirable elements that we can replicate here?

IATA would like to highlight three initiatives that may be of interest to homeland security officials in the United States as they evaluate next-generation screening measures. We find these to be solid examples of industry and government working in partnership.

1) UK Better Regulation for Aviation Security Initiative: Proposal for a new outcome focused, risk-based approach to regulation which builds on the similar approach used for aviation safety. IATA believes that such a regulatory structure can serve as a solid foundation for next generation passenger screening.
2) Canada: Trusted Traveller CATSA Screening Line: Passenger checkpoint optimization that creates a special security lane for holders of the NEXUS card. The program will be live at all Class 1 trans-border airports by mid-February 2012. Such known traveler programs serve as a cornerstone for next-generation checkpoints.
3) ICAO: Next Generation Passenger Screening Technical Advisory Group: Chartered by ICAO and including representatives of 19 member states, including the U.S., this group is tasked to examine issues related to a future passenger screening checkpoint including, but not limited to, costs, infrastructure and processes. IATA would encourage the continued active participation of the U.S.

67123.975

Post-Hearing Questions for the Record
Submitted to Charles M. Barclay
From Senator Joseph I. Lieberman

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1.) A trusted traveler program could increase security by allowing TSA to focus its limited resources on the highest risk passengers. But it cannot compromise security and must ensure passengers that opt to enroll in TSA's Pre-Check Pilot are in fact trusted travelers.

A government approved identification document presented to TSA may be valid, but it may not belong to the passenger who is presenting it. Should these trusted travelers have to provide further confirmation to TSA that they are who they say they are, with a biometric identification?

Yes, biometric identification for trusted travelers must eventually be a part of PreCheck or any subsequent trusted traveler programs. The Registered Traveler program, which included participation from 250,000 individuals at 22 airports, included a biometric element, so the concept has already been tested in the field, and there is no doubt that security is strengthened by the utilization of biometrics.

With that said, we believe there is value in moving forward with the pilot approach that is now underway with the PreCheck program. Although the program as it currently operates does not include biometric elements or requirements, the current boarding pass model is a good first step. In the future, biometrics and a biometric verification process can and should be added to ensure identiy verification. From the perspective of airport executives, it is important to move forward with the trusted traveler program as Administrator Pistole and his team have designed it, recognizing that biometrics can and should be a part of our long-term trusted traveler approach.

If the program is voluntary, should TSA consider using additional data, even commercial data if a passenger will agree to it, to inform decisions regarding trusted travelers?

Yes, AAAE supports the utilization of commercial data and any other data that can enhance program and aviation system security. It is our understanding that federal privacy laws prohibit the federal government from accessing commercial data, a fact which necessitates effective partnership and coordination with the private sector. The federal government and the private sector were able to partner effectively as part of the Registered Traveler program in a way that allowed for the utilization of commercial data while protecting important

67123.976

privacy considerations and in accordance with federal law. That experience offers an important model for moving forward with future trusted traveler programs.

2.) You testified in support of TSA's initial steps to pilot some risk-screening programs, which are important but modest steps forward designed to test new ideas. How would you suggest DHS and TSA scale up or build upon these initial risk-based screening programs?

To take full advantage of the security and efficiency benefits that PreCheck or similar trusted traveler programs offer, participation must evolve beyond elite fliers on particular air carriers to a wider qualified pool of travelers and become community-based and airport centric. After all, most qualified travelers will expect and demand that they will be able to use the program at a participating airport regardless of the specific carrier they are flying. Travelers also will obviously expect that the program is available at as many airports as possible.

Fortunately, experiences with the Registered Traveler Program offer an important roadmap on how to quickly and effectively enroll eligible populations and provide some of the additional requirements – including effective queue management – that are necessary to make PreCheck or other trusted traveler programs a success.

With the Registered Traveler Program, 250,000 people were enrolled in a relatively short time and the program quickly became operational at 22 airports across the country. Although the business model with Registered Traveler ultimately proved unsuccessful, the effort was incredibly successful operationally and should serve as a model for moving forward to grow the program efficiently and effectively.

Moving forward, TSA must continue to work closely with the airport community to marry federal resources and requirements with local knowledge and expertise. AAAE has established a Security Task Force that is actively involved in discussions with the agency to move in that direction, and we are optimistic that the effort will produce tangible results soon. The AAAE Security Task Force is also working collaboratively with TSA to address issues related to checkpoint configuration, queue management, modified LEO response expectations and public communications to ensure that ongoing efforts to grow and improve trusted traveler programs are successful.

3.) Do you believe that TSA, airlines, and local airport and law enforcement authorities should reexamine their relationships and authorities at and near the checkpoint? How could this improve efficiency or mitigate confusion, or why might we need to continue to differentiate between TSA and local authority at the checkpoint?

Yes, a reexamination of the relationship and authorities among TSA, airlines, and airport operators at screening checkpoints is appropriate. In our view, airport operators must be given the primary authority to address and manage the queuing process at screening checkpoints. By giving the airport control and responsibility for this parts of the process, we can ensure consistency and efficiency and avoid the pitfalls associated with airline affinity-based queuing, which docs not allow for the broad based utilization of screening assets.

Post-Hearing Questions for the Record
Submitted to Charles M. Barclay
From Senator Thomas R. Carper

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1. In your testimony, you discussed how the current "one-size-fits all" screening process at our airports does not meet the needs of the traveling public and that we should look at moving to a system that detects dangerous people instead of only dangers things. As you know, this Committee has continually challenged government officials to work smarter with federal dollars and to find efficiencies in our government programs without compromising security. To this end, I understand the Transportation Security Administration (TSA) has developed a pilot to help expedite the flow trusted travelers, but there is still much room for growth. Can you discuss the challenges TSA may face as it looks to expand the pilot and how industry can help find solutions to these issues?

AAAE is very supportive of TSA's efforts to move forward with its voluntary passenger pre-screening initiative known as PreCheck, and we believe the effort holds huge promise in more effectively targeting limited screening resources at airport screening checkpoints. Airport executives anticipate great success with the program and believe that the next challenge will be moving from a small, largely airline-centric program in operation at a limited number of airports to one that is operational for large numbers of qualified travelers at airport facilities across the country.

To take full advantage of the security and efficiency benefits that PreCheck or similar trusted traveler programs offer, participation must evolve beyond elite fliers on particular air carriers to a wider qualified pool of travelers and become community-based and airport centric. After all, most qualified travelers will expect and demand that they will be able to use the program at a participating airport regardless of the specific carrier they are flying. Travelers also will obviously expect that the program is available at as many airports as possible.

The good news is that we already have a model – with the Registered Traveler Program – for how to quickly and effectively enroll eligible populations and provide some of the additional requirements – including effective queue management – that are necessary to make PreCheck or other trusted traveler programs a success.

With the Registered Traveler Program, 250,000 people were enrolled in a relatively short time and the program quickly became operational at 22 airports across the country. Although the business model with Registered Traveler ultimately proved unsuccessful, the effort was incredibly successful operationally and should serve as the roadmap for moving forward to grow the program efficiently and effectively.

Moving forward, TSA must continue to work closely with the airport community to marry federal resources and requirements with local knowledge and expertise. AAAE has established a Security Task Force that is actively involved in discussions with the agency to move in that direction, and we are optimistic that the effort will produce tangible results soon. The AAAE Security Task Force is also working collaboratively with TSA to address issues related to checkpoint configuration, queue management, modified LEO response expectations and public communications to ensure that ongoing efforts to grow and improve trusted traveler programs are successful.

67123.978

Post-Hearing Questions for the Record
Submitted to Charles M. Barclay
From Senator Mary L. Landrieu

"Ten Years After 9/11: The Next Wave in Aviation Security"
November 2, 2011

1. The U.S. Travel Association has recommended the establishment of a Trusted Traveler Program, and TSA's Pre-Check pilot program launched last month represents this administration's attempt to create one. Mr. Dow's testimony suggested that the program must significantly improve traveler convenience in order to incentivize large-scale enrollment. After all, program participants are required to undergo a background check and register their biometric data with TSA in order to qualify, so it is important to consider what they stand to gain in return for their troubles. Do you feel that TSA's Pre-Check program provides a sufficient degree of incentives? What changes would you suggest to further incentivize enrollment?

While AAAE is very supportive of TSA's efforts to move forward with its voluntary passenger pre-screening initiative known as PreCheck, it is clear that the initial effort – which is largely limited to elite airline fliers – lacks sufficient incentives for a wide-scale deployment. To take full advantage of the security and efficiency benefits that PreCheck or similar trusted traveler programs offer, participation must evolve beyond elite fliers on particular air carriers to a wider qualified pool of travelers and become community-based and airport centric. After all, most qualified travelers will expect and demand that they will be able to use the program at a participating airport regardless of the specific carrier they are flying. Travelers also will obviously expect that the program is available at as many airports as possible.

Fortunately, experiences with the Registered Traveler Program offer an important roadmap on how to quickly and effectively enroll eligible populations and provide some of the additional requirements – including effective queue management – that are necessary to make PreCheck or other trusted traveler programs a success. With the Registered Traveler Program, 250,000 people were enrolled in a relatively short time and the program quickly became operational at 22 airports across the country. Although the business model with Registered Traveler ultimately proved unsuccessful, the effort was incredibly successful operationally and should serve as a model for moving forward to grow the program efficiently and effectively.

Moving forward, TSA must continue to work closely with the airport community to marry federal resources and requirements with local knowledge and expertise. AAAE has established a Security Task Force that is actively involved in discussions with the agency to move in that direction, and we are optimistic that the effort will produce tangible results soon. The AAAE Security Task Force is also working

67123.979

collaboratively with TSA to address issues related to checkpoint configuration, queue management, modified LEO response expectations and public communications to ensure that ongoing efforts to grow and improve trusted traveler programs are successful.

2. I am interested in the process airports use to screen new hires as well as the access control measures that exist within the airport to prevent workers from bringing dangerous items into sensitive areas like the tarmac or cargo holds. Please describe screening and access control procedures for airport employees and the respective role of airport security officials and the TSA.

As public entities, airports provide a critical local layer of security and perform a number of inherently local security-related functions at their facilities, including credentialing and access control. These duties, which have been local responsibilities for decades, are performed by local authorities in accordance with federal standards and subject to federal review and continuous oversight. Airport executives believe strongly that those responsibilities must remain in local hands to maintain a critical layer of security that has been in place for decades.

With regard to efforts being undertaken by airports to prevent workers from bringing dangerous items into sensitive areas like tarmacs or aircraft cargo holds, the possibility of an inside threat is something that airports take very seriously and have worked collaboratively with TSA to address. In recent years, airports and TSA have implemented a multi-faceted plan that includes behavior recognition programs, security awareness training for employees, targeted physical inspection of airport workers, enhanced access control measures, and the deployment of additional technology.

Additionally, and perhaps more importantly, a vigorous system is in place to identify dangerous people and prevent them from ever having access to sensitive airport areas in the first place. After all, the airport environment is full of potentially dangerous things from fuel trucks to tools to weapons in checked luggage that pose a threat to the system in the wrong hands.

Prior to ever receiving a badge granting access to sensitive airport areas, an individual is subject to federal background checks including a fingerprint-based criminal history record check performed by the Federal Bureau of Investigation and a Security Threat Assessment conducted by TSA. While the federal government holds sole responsibility for performing those necessary and required checks for prospective aviation workers, airports provide an extra layer of security through local adjudication of the background checks. Additionally, airports operate and manage enrollment, credentialing, badging, and access control systems locally in accordance with strict federal standards. The current system for aviation workers strikes the proper balance between the local government's need for operational efficiency and the federal government's need to set standards, maintain strict oversight, and perform critical federal vetting functions.

○

67123.980