AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 111–1070

INTELLIGENCE REFORM—2010

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

OF THE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JANUARY 20, 2010
INTELLIGENCE REFORM: THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK—PART I

JANUARY 26, 2010
INTELLIGENCE REFORM: THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK—PART II

MARCH 10, 2010
THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: WATCHLISTING AND PRE-SCREENING

MARCH 17, 2010
THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: INTELLIGENCE REFORM AND INTERAGENCY INTEGRATION

APRIL 21, 2010
THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: SECURING THE VISA PROCESS

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

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

INTELLIGENCE REFORM—2010

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00002 Fmt 6019 Sfmt 6019 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

S. Hrg. 111–1070

INTELLIGENCE REFORM—2010

HEARINGS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

OF THE

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JANUARY 20, 2010
INTELLIGENCE REFORM: THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK—PART I

JANUARY 26, 2010
INTELLIGENCE REFORM: THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK—PART II

MARCH 10, 2010
THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: WATCHLISTING AND PRE-SCREENING

MARCH 17, 2010
THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: INTELLIGENCE REFORM AND INTERAGENCY INTEGRATION

APRIL 21, 2010
THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: SECURING THE VISA PROCESS

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

56–838 PDF WASHINGTON : 2011

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

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
ROLAND W. BURRIS, Illinois
PAUL G. KIRK, JR., Massachusetts*
EDWARD E. KAUFMAN, Delaware*

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
SCOTT P. BROWN, Massachusetts**
JOHN McCAIN, Arizona
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada
LINDSEY GRAHAM, South Carolina
ROBERT F. BENNETT, Utah**

MICHAEL L. ALEXANDER, *Staff Director*
CHRISTIAN J. BECKNER, *Professional Staff Member*
JEFFREY E. GREENE, *Counsel*
SEAMUS A. HUGHES, *Professional Staff Member*
GORDON N. LEDERMAN, *Counsel*
BLAS NUNEZ-NETO, *Professional Staff Member*
JASON M. YANUSSI, *Professional Staff Member*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
ROBERT L. STRAYER, *Minority Director of Homeland Security Affairs*
IVY A. JOHNSON, *Minority Deputy General Counsel*
JOHN K. GRANT, *Minority Counsel*
LUKE P. BELLOCCHI, *Minority Counsel*
MATTHEW L. HANNA, *Minority CBP Detailee*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*
LAURA W. KILBRIDE, *Hearing Clerk*

*Senator Kaufman replaced Senator Kirk on the Committee effective March 9, 2010.

**Senator Brown replaced Senator Bennett on the Committee effective March 9, 2010.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00004 Fmt 5904 Sfmt 5904 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

CONTENTS

	Page
Opening statements:	
Senator Lieberman	1, 49, 81, 119, 153
Senator Collins	3, 51, 83, 121, 155
Senator Tester	17
Senator Burris	20, 74
Senator McCain	22, 68, 173
Senator Ensign	24
Senator Coburn	27
Senator Akaka	30
Senator Levin	32
Senator McCaskill	35
Senator Carper	37, 65, 104, 136, 176
Senator Bennett	70
Senator Kirk	72
Senator Brown	85
Senator Voinovich	170
Prepared statements:	
Senator Lieberman	185, 284, 301, 355, 453
Senator Collins	188, 287, 303, 357, 456
Senator Carper	305

WITNESSES

WEDNESDAY, JANUARY 20, 2010

Hon. Michael E. Leiter, Director, National Counterterrorism Center, Office of the Director of National Intelligence 5
Hon. Dennis C. Blair, Director of National Intelligence, Office of the Director of National Intelligence 7
Hon. Janet A. Napolitano, Secretary, U.S. Department of Homeland Security 9

TUESDAY, JANUARY 26, 2010

Hon. Thomas H. Kean, Former Chairman, National Commission on Terrorist Attacks Upon the United States, and Hon. Lee H. Hamilton, Former Vice Chairman, National Commission on Terrorist Attacks Upon the United States 54

WEDNESDAY, MARCH 10, 2010

Russell E. Travers, Deputy Director, Information Sharing and Knowledge Development, National Counterterrorism Center, Office of the Director of National Intelligence 86
Timothy J. Healy, Director, Terrorist Screening Center, Federal Bureau of Investigation, U.S. Department of Justice 88
Gale D. Rossides, Acting Administrator, Transportation Security Administration, U.S. Department of Homeland Security 90
David V. Aguilar, Acting Deputy Commissioner, U.S. Customs and Border Protection, U.S. Department of Homeland Security 93

WEDNESDAY, MARCH 17, 2010

Hon. Benjamin A. Powell, Former General Counsel of the Office of the Director of National Intelligence (2006–2009) 122
Hon. Jeffrey H. Smith, Former General Counsel of the Central Intelligence Agency (1995–1996) 125

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00005 Fmt 5904 Sfmt 5904 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

Page

Richard Nelson, Senior Fellow and Director, Homeland Security and Counterterrorism Program, Center for Strategic and International Studies 127

WEDNESDAY, APRIL 21, 2010

Hon. David F. Heyman, Assistant Secretary, Office of Policy, U.S. Department of Homeland Security 157
Hon. Janice L. Jacobs, Assistant Secretary, Bureau of Consular Affairs, U.S. Department of State 159
Hon. John T. Morton, Assistant Secretary, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security 164

ALPHABETICAL LIST OF WITNESSES

Aguilar, David V.:
Testimony 93
Prepared statement 328
Blair, Hon. Dennis C.:
Testimony 7
Joint prepared statement with Mr. Leiter 191
Hamilton, Hon. Lee H.:
Testimony 54
Joint prepared statement with Mr. Kean 290
Healy, Timothy J.:
Testimony 88
Prepared statement 310
Heyman, Hon. David F.:
Testimony 157
Prepared statement 458
Jacobs, Hon. Janice L.:
Testimony 159
Prepared statement 465
Kean, Hon. Thomas H.:
Testimony 54
Joint prepared statement with Mr. Hamilton 290
Leiter, Hon. Michael E.:
Testimony 5
Joint prepared statement with Mr. Blair 191
Morton, Hon. John T.:
Testimony 164
Prepared statement 475
Napolitano, Hon. Janet A.:
Testimony 9
Prepared statement 200
Nelson, Richard:
Testimony 127
Prepared statement 445
Powell, Hon. Benjamin A.:
Testimony 122
Prepared statement with attachments 359
Rossides, Gale D.:
Testimony 90
Prepared statement 316
Smith, Hon. Jeffrey H.:
Testimony 125
Prepared statement 427
Travers, Russell E.:
Testimony 86
Prepared statement 306

APPENDIX

JANUARY 20, 2010

Statement for the Record submitted by Mr. Blair 214
Document titled "Office of the Director of National Intelligence Instruction No. 80.05," submitted by Mr. Leiter and Mr. Blair for the Record 215
American Civil Liberties Union (ACLU), prepared statement 234

Page

Responses to post-hearing questions for the Record from:
Mr. Leiter 245
Mr. Blair 251
Secretary Napolitano 255

JANUARY 26, 2010

Responses to post-hearing questions for the Record from:
Mr. Kean and Mr. Hamilton 298

MARCH 10, 2010

Responses to post-hearing questions for the Record from:
Mr. Travers 338
Ms. Rossides and Mr. Aguilar 339

MARCH 17, 2010

Responses to post-hearing questions for the Record from:
Mr. Smith 452

APRIL 21, 2010

Responses to post-hearing questions for the Record from:
Mr. Heyman and Mr. Morton 484
Ms. Jacobs 515

INTELLIGENCE REFORM: THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK—PART I

WEDNESDAY, JANUARY 20, 2010

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, Levin, Akaka, Carper, Pryor, McCaskill, Tester, Burris, Collins, Coburn, McCain, Ensign, and Bennett.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning and welcome to the hearing. As we all know, on this past Christmas Day, December 25, 2009, Umar Farouk Abdulmutallab slipped through the multi-layered defenses we have erected since September 11, 2001, to stop attacks against our homeland and boarded Northwest Flight 253 from Amsterdam to Detroit over which he attempted a suicide bombing. A faulty detonator and courageous and quick action by the passengers and crew prevented the deaths of 290 people on board that plane and many more on the ground below. We were very lucky.

Because it has now been 5 years since the enactment of the 9/11 Commission recommendations for intelligence reform, Senator Collins and I decided last year to initiate a series of oversight hearings this year to examine how well these reforms have been implemented and whether further changes in the law, regulation, or implementation are needed to protect our country. That is, in fact, the inquiry we begin today, but now, of course, we must carry out our oversight responsibilities through the unsettling prism of the Christmas Day breach of our homeland defenses by the terrorist Abdulmutallab.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which is commonly known as the "9/11 Commission Act," was the most sweeping intelligence reform since the creation of the Central Intelligence Agency (CIA) more than 50 years earlier. Among its many significant improvements, the 9/11 Commission Act established a Director of National Intelligence (DNI) to integrate our 16 intelligence agencies. It also created the National

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00009 Fmt 6633 Sfmt 6633 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

Counterterrorism Center (NCTC) 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.

Earlier, in 2002, our government's failures on September 11, 2001, also moved Congress to act on recommendations to create a Department of Homeland Security (DHS) to better cope with the threats our country would face in the 21st Century. I believe these post-September 11, 2001, reforms have worked very well. The record shows that after the creation of the Department of Homeland Security in 2002 and the establishment of the DNI and National Counterterrorism Center in 2004, there was not a terrorist attack by Islamist extremists on America's homeland for almost 7 years. No one would have predicted that on September 12, 2001. So we have a lot to be grateful for.

Some of the most successful defenses of our homeland, in my opinion, have been truly amazing, although the details of these, of necessity, remain largely unknown. Two of the most impressive of those successful defenses of our homeland occurring in 2009 with regard to Najibullah Zazi and David Headley. One of the most impressive cases to me was the Zazi case, he was arrested last September with the plans and materials needed for devastating bombing attacks on New York City. This was the most dangerous terrorist plot on our soil since September 11, 2001, dangerous in the sense of the consequences it would have had, and it was only stopped by brilliant, courageous, and cooperative work by our intelligence, law enforcement, and homeland security agencies.

Senator Collins and I, and other Members of this Committee and other committees, have been briefed on the details, but everything worked just as we hoped it would when we adopted the post-September 11, 2001, legislation. There was remarkable agility, brilliant judgment, and total cooperation between intelligence, homeland security, and law enforcement communities both here within the United States and throughout the world.

Notwithstanding these remarkable achievements over the 7 years after the enactment of the Department of Homeland Security and some of the extraordinary defenses in the Headley and Zazi cases, which occurred in 2009, the record also shows that in 2009 three Islamist terrorists broke through our defenses: Carlos Bledsoe, who murdered a U.S. Army recruiter in Little Rock, Arkansas, in June, simply because he was wearing the uniform of the U.S. Army; Nidal Hasan, who murdered 13 Americans at Fort Hood in November; and Umar Farouk Abdulmutallab, who would have killed hundreds more if the explosive he had hidden in his clothing on Christmas Day had worked. So, clearly, there are some things about our homeland defenses that are not working as we need them to, and we have to find out together what is going wrong and why and then fix it.

I know it is probably not realistic to promise the American people that we will stop every attempted terrorist attack on our homeland, but I feel very strongly that must be our goal. It certainly is the standard that will guide our Committee in this inquiry and the other we are conducting on the terrorist attack at Fort Hood and any recommendations for Executive or Legislative action that we make as a result of our inquiry.

Our purpose is to review the current state of our homeland security through these cases and to make recommendations for reform that will get our homeland—America—as close as possible to 100-percent security from terrorist attacks.

In the Christmas Day bombing case, there was so much intelligence and information available to our government that pointed to Abdulmutallab's violent intentions that it is beyond frustrating—it is infuriating—that this terrorist was able to get on that plane to Detroit with explosives on his body. He was able to do so, in sum, as President Obama has correctly said, because of systemic failures and human errors.

Our responsibility is clear: We have to find what the systemic failures were and fix them, and if the Administration or we, in our deliberations, find that there were personnel of the Federal Government who did not perform up to the requirement of their jobs in these cases, they should be disciplined or removed.

As is clear from the Christmas Day attack which almost killed hundreds, the Fort Hood attack which did kill 13, and the thwarting of the Zazi plot that saved countless American lives, the decisions of the public servants who work to protect us from terrorists every day have life-and-death consequences. If we do not hold accountable those who made these human errors, the probability is greater that they will be made again.

I have not called this hearing along with Senator Collins to knock down the new walls of homeland security that we built after September 11, 2001. We have called it to repair and reinforce them so that they better protect the American people from terrorist attack. It is in that spirit that I thank our witnesses, the Director of the National Counterterrorism Center, Michael Leiter; the Director of National Intelligence, Admiral Dennis Blair; and the Secretary of Homeland Security, Janet Napolitano, for being with us today. I look forward to your testimony and the questions and answers that will follow.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Every day the men and women of our military, homeland security, law enforcement, and intelligence community work hard to keep our Nation safe. They serve on the front lines of the war against terrorism, and over the last year alone, their efforts have helped thwart numerous terrorist attacks.

But as the attempted Christmas Day attack demonstrates, our government's efforts to detect and disrupt terrorist plots must be strengthened.

We dodged a bullet in the skies above Detroit on Christmas Day. A mere fluke—a mistake by the terrorist on that plane or a failed detonator—prevented that attack from succeeding. The quick action of courageous passengers and crew helped spare the lives of nearly 300 passengers on Flight 253.

We cannot escape the cold, hard facts. Terrorists have not relented in their fanatical quest to frighten our Nation's citizens and to slaughter as many Americans as possible. Their tactics continue to evolve. Attacks inspired by al-Qaeda's violent ideology, including

those by lone wolves or those perpetrated by smaller uncoordinated cells, are incredibly difficult to detect. The threat posed by America's enemies continues to grow, and our Nation's efforts to defeat them must be nimble, determined, and resilient.

In response to the terrorist attacks of September 11, 2001, this Committee offered the most sweeping reform for the intelligence community since the Second World War. The Intelligence Reform and Terrorist Prevention Act of 2004 did much to improve the management and performance of our intelligence, homeland security, and law enforcement agencies. The increased collaboration and information sharing have helped our Nation prevent numerous attacks, at least nine in the last year alone.

But reform is not a destination. It is a work in progress. Reform requires constant focus and attention to stay a step ahead of the threats we face.

For example, despite the considerable improvements in information sharing, our intelligence community continues to rely on internal systems and processes that are relics from the days before reform. These systems did not effectively surface intelligence information so that analysts and security officials can effectively identify threats in real time.

The President has asserted—and I agree—that there was ample credible intelligence on Abdulmutallab to warrant his inclusion on the No Fly List, yet that did not occur even though his own father warned U.S. officials about his ties to Islamist extremists. Whether this failure was caused by human error, poor judgment, outmoded systems, or the sheer volume of data that must be analyzed, we simply must develop systems and protocols to prevent these failures.

Consider what I believe to be the most obvious error in handling Abdulmutallab's case. After his Islamist extremist connections in Yemen were reported by his father, the State Department should have revoked his visa. At the very least, he should have been required to report to our embassy and explain his activities and answer questions before he was allowed to retain his visa.

The State Department has this authority. In fact, our law, the Intelligence Reform Act, protects the State Department from lawsuits when its officials revoke a visa overseas. But the State Department failed to act. Most disturbing, the State Department is also pointing fingers at other agencies to explain this failure.

The President has now directed the intelligence community to determine which of the 400,000 suspected terrorists in the Terrorist Screening Center's watchlist have valid U.S. visas. But that response is not sufficient.

The government should immediately identify and suspend the visas of all persons listed in the broadest terrorist database operated by the NCTC, known as the Terrorist Identities Datamart Environment (TIDE) list, until a further investigation is undertaken in each case. These visa holders with suspected connections to terrorism should shoulder the burden of proving that they do not intend to harm this Nation or its citizens, and if they cannot meet this burden, then we cannot take the risk of permitting them the privilege of traveling to our country.

But immediately revoking the visas of suspected terrorists is only the first step. The Department of Homeland Security has an obligation to confirm the validity of visas held by every foreign passenger. This is done only in some airports now. Instead, what happens now is that confirmation of valid visas only occurs once the passengers have arrived on our land. There is no technological reason why this cannot occur.

We did not choose this war. It was thrust upon us by terrorists who are determined to destroy our way of life. Our counterterrorism efforts must be tireless and steadfast. We must continue to build on the intelligence reforms already in place to make America more secure. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins. Let us begin the testimony with Michael Leiter, who is the Director of the National Counterterrorism Center. Thanks for being here.

TESTIMONY OF HON. MICHAEL E. LEITER,[1] DIRECTOR, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. LEITER. It is my pleasure, Chairman Lieberman, Ranking Member Collins, and Members of the Committee. It is a privilege to appear before this Committee—again, the Committee that was most instrumental in reforming the intelligence community and creating the NCTC.

To open, I want to offer what I hope is an absolutely crystal-clear assertion: Umar Farouk Abdulmutallab should not have stepped onto a plane on Christmas Day. The counterterrorism system collectively failed, and I, along with Director Blair and Secretary Napolitano and others, want to tell you and the American people the same thing we told the President: That we have to do better.

As one of several attacks, several of which you cited, we have been reminded again how unceasing our enemy is and how committed they are to attacking the United States and how committed we have to be in protecting Americans.

To begin, I would like to give a short rundown of the bombing attempt and try to tell you from our perspective what we did miss. And I want to start by debunking what has become conventional wisdom to some, which is that this failure was just like September 11, 2001. And, in fact, it was not. Now, that does not make the failure any less significant, but it does mean that the solutions might be very different from what we approach in our reforms post-September 11, 2001.

It was not a failure to share intelligence. Instead, it was a failure to connect, integrate, and fully understand the intelligence that we had collected. Although NCTC and the intelligence community have long warned about the threat posed by al-Qaeda in the Arabian Peninsula, as I did in the fall before this Committee, we did not correlate the specific information that would have identified Abdulmutallab and kept him off that flight on Christmas Day.

More specifically, the intelligence community, as I said, had highlighted the growing character of al-Qaeda in Yemen and the

[1] The joint prepared statement of Mr. Leiter and Mr. Blair appears in the Appendix on page 191.

potential for it to strike targets not just in Yemen, but the possibility of reaching beyond Yemen to the homeland. And we also analyzed information that al-Qaeda in the Arabian Peninsula (AQAP), was working with an individual who only after the fact did we realize was, in fact, Abdulmutallab. And I would also note that the intelligence community repeatedly warned of the type of explosive device throughout the fall that was used by Abdulmutallab in this attack, and the ways in which it might prove challenging to screening in, of course, the way it did in Amsterdam.

But despite all of that and the overall themes that we identified, again, we failed to make the final connections—the last tactical mile that linked Abdulmutallab's identity to this plot. We had the information that came from his father saying that he was concerned that his son had, in fact, gone to Yemen, that he was coming under the influence of unknown religious extremists, and that he was planning not to return home. And we also had other streams of information coming from other intelligence channels that provided different pieces of the story. We had a partial name—Umar Farouk; we had the indication of a Nigerian; but there was no single piece of intelligence that brought that all together, nor did our analysts at NCTC or elsewhere bring that information together.

As a result, as you have both noted, although Abdulmutallab was identified as a known or suspected terrorist and his name was entered into our database, the Terrorist Identities Datamart Environment, the derogatory information that we associated with him at the time did not meet existing policy standards—those that were adopted in 2008 and promulgated in 2009—for him to be watchlisted, let alone placed on the No Fly List or Selectee Lists.

But let me be clear again. Had all of the information the United States had available been linked together, his name undoubtedly would have been watchlisted, and, thus, he would have been on the visa screening list and the border inspection list. And whether he would have been placed on the No Fly or Selectee List then, would have been based on the existing strength of the analytic judgments at the time. And as I have already noted, one of the clear lessons that I think we have learned is the need, as the President has directed us to do, to re-examine those standards for inclusion in those critical lists before people reach our borders.

Finally, Mr. Chairman, Senator Collins, and Members, without trying to make any excuses for what we did not do—because as I think I have already stated, as I hope I have made clear, we did not do things well and we did not do things right—I do think it is critical that we note some context in which this failure occurred. And I thank you for your kind words for the intelligence community, NCTC, law enforcement, and homeland security in noting some of the successes. But we have to have more successes.

Each day NCTC receives literally thousands of pieces of intelligence related to terrorism. I will tell you it is more than 5,000 pieces a day that flow into our center, and we review literally thousands of names each day—again, more than 5,000 names a day that we review. And every day we place more than 350 people on the watchlist. So although in hindsight we can assess with a very high degree of confidence that Abdulmutallab was, in fact, bonding

with AQAP, we did not do it at the time. Although we must and will do better—because I believe we have the people who will make sure we do better—we must recognize, as the Chairman did, that there is no silver bullet. And, in fact, as the terrorist threat becomes more nimble and more multi-dimensional, as illustrated by the threats we have seen over the past year, we as well have to have a multi-dimensional, multi-layered set of defenses—intelligence, technology, international cooperation, law enforcement, and military—to keep our Nation as safe as possible.

With that, I will turn the microphone over to Director Blair, but I do look forward to answering the Committee's questions and, most importantly, I look forward to getting the Committee's guidance on how you believe we can improve the system that we have. Thank you.

Chairman LIEBERMAN. Thanks, Director Leiter.

Admiral Blair, it is encouraging that your cooperation has even gone to your testimony before this Committee. Thank you.

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

Mr. BLAIR. Sir, I am glad to be here to talk about this because you need to know and the American people need to know what we are doing and what we need to do, and so thank you for inviting me to talk with you this morning.

Let me echo Director Leiter's words that Umar Farouk Abdulmutallab should not have stepped on Northwest Flight 253 for Detroit. The overall counterterrorism system did not do its job. It is in large part my responsibility. I told the President that I and the other leaders of the intelligence community are determined to do better in the future.

And you have heard from Director Leiter the sequence of events, and you would be correct to conclude that the system that existed to protect the country was capable of stopping this attack, but it did not do so in this case for a set of reasons that I think we understand and that we are working right now to fix.

And I should make it clear to this Committee that a lot of the responsibility for pushing us forward in this area, that the system we now have, was due in great measure to the Intelligence Reform and Terrorism Prevention Act of 2004, which created my position, the National Counterterrorism Center, and other key parts of the system, such as the Terrorist Identities Datamart Environment; the watchlists, including the No Fly List; aggressive collection and analysis against terrorist threats; and a great improvement in sharing intelligence information across both the intelligence community and the entire government. So we should not underrate the progress of the past as we move forward. But the threat is also evolving, and I would say we have a good capability to detect and disrupt these sort of multi-purpose teams that take months to plan, rehearse, fund, provide the logistics support for, and attack.

[1] The joint prepared statement of Mr. Blair and Mr. Leiter appears in the Appendix on page 191.

But we are not as capable as we should be of carrying out the much more difficult task of detecting these self-radicalized citizens of the United States, Europe, and other countries like Nigeria, who are given a very simple mission and an advanced bomb to carry it out, or who plan their own attacks inspired by al-Qaeda's message but not directed by al-Qaeda.

Last year, as you mentioned, Mr. Chairman, we stopped Zazi. We also stopped Michael Finton and Hosam Smadi. But Hasan and Bledsoe we did not stop, and as you said, we were lucky with Abdulmutallab. So we have to improve our intelligence system further so that we can identify and stop these lone contacts with a minimum of communication and, frankly, with a lot more knowledge of how our system works due to the public discussion of it that is taking place.

And as Secretary Napolitano will tell you, we have to improve not just the intelligence component of this but the active defenses which we have, some of which depend on intelligence, but some of which cannot depend on intelligence.

So what are the improvements that we are making based on this incident and the other things that we have learned over the course of recent years? They really fall into four categories. They are currently underway, but we will continue to refine them and work on them both in the short term and certainly over the long term.

First, changing the way we apply these no-fly criteria so that they are less restrictive, more flexible, while at the same time they continue to protect the civil liberties of U.S. persons. The no-fly criteria that we were working under on December 24 of last year had been arrived at by a bureaucratic process that stretched across two Administrations. It started in the summer of 2008. They were implemented just before this Administration came in and were reaffirmed by this Administration, and they were, frankly, a too legalistic and rote process rather than having the flexibility to react to the situation, which they really needed. And we have fixed that, and that is very important.

Second, I need to assign more clearly defined responsibilities for analysis and follow-up of the information we now have. Frankly, we had a situation in which everybody was responsible for working, everybody had the dots to connect, but I had not made it clear exactly who had primary responsibility, who had secondary responsibility, so when the time crunch comes the people know who cannot go home at night until they carry that out while other people are working on other things.

Third, we have to have an ability—and we are doing so—to adjust the resources as the threat shifts. As Director Leiter said, we had strategic warning of al-Qaeda in the Arabian Peninsula's intent to send operatives outside of Yemen, and yet I allowed the analytical resources focusing on Yemen to focus more on the internal Yemen problem, where we also had active threats to Americans and to American interests. We did not add more resources, shift the emphasis, ensure that both priorities were covered, and we need to do so. We are doing so. We are adding resources immediately, and we are setting up a system so that we can adjust more to threats.

And, fourth—you have alluded to this, Mr. Chairman and Senator Collins—we have to improve both the technical and the human ability to deal with this massive information that our terrorist analysts must distill to enable them to provide tactical level warning on individuals, which is a very tough task. And although we have used a lot of technical tools in recent years, we have put them in. Some were outdated, as you said, Senator Collins. We have a priority effort to re-examine those, make sure that we are going with the best that is available. We are using both outside experts as well as those that we have inside.

These improvements that we are making are not years in the making. We are working on them now. We have already made improvements in the 3 weeks since that attack. We have a press on them for getting short-term ones done immediately, and, more importantly, we will continue to work them dynamically over time rather than waiting for artificial deadlines to take place. And I have also convened a panel of outside experts that will both review exactly what happened in the December case. We have done preliminary inquiries, but we need to take a more careful look, and also it will review the changes we are making to see if we are getting it right, to tell us what we are not doing that we should do.

It is important—and I share your goal, Mr. Chairman, about the 100-percent goal that we shoot for, but we have to make it clear that we cannot give an absolute guarantee of identifying every single one of these terrorists. We need a system of offense and defense, go after them where they are, push our intelligence on all points, and then have defenses that are strengthened by intelligence but do not completely depend on it in order to defend our citizens. And we are dedicated to pushing toward that 100-percent goal as quickly and with as much determination as we can.

Thank you, Mr. Chairman. I turn it over to Secretary Napolitano.

Chairman LIEBERMAN. Thanks, Director Blair. Secretary Napolitano, good morning.

TESTIMONY OF HON. JANET A. NAPOLITANO,[1] SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Good morning, Chairman Lieberman, Senator Collins, and Members of the Committee. Thank you for this opportunity to testify on the terrorist attack aboard Northwest Flight 253 on Christmas Day. I am pleased to be here today with my colleagues Admiral Blair and Director Leiter.

As President Obama has made clear, this Administration is determined to find and to fix the vulnerabilities in our systems that allowed this attack to occur. Our country's efforts against terrorism include the actions of DHS and of many other agencies, as well as those of our international allies.

I would like to take a moment to explain and describe the DHS role in securing air travel.

First, DHS is and can be characterized as a consumer of the U.S. Government's consolidated terrorist watchlists which we use to help keep potential terrorists from boarding flights and to identify travelers who should undergo additional screening. Within the

[1] The prepared statement of Secretary Napolitano appears in the Appendix on page 200.

United States, DHS performs the actual physical screening at airport checkpoints and provides further in-flight security measures. Outside the United States, DHS works with foreign governments and airlines to advise them on which passengers may prove a threat and required security measures for flights inbound to the United States. Transportation Security Administration (TSA), of course, does not screen people or baggage at international airports.

Regarding the Christmas Day attack, Umar Abdulmutallab should never have been allowed to board this U.S.-bound plane with explosives. The interagency process to fix these vulnerabilities is well underway, and we are all working on it jointly.

We welcome, at the Department, the opportunity offered by the process described by Admiral Blair and Director Leiter to contribute to improving the Federal Government's ability to connect and assimilate intelligence, and we appreciate the work that they have done and the ongoing relationship that we have.

We are also focused on improving aviation screening and expanding international partnerships to guard against a similar type of attack. I have submitted a longer written statement describing the various DHS programs that are at work to keep terrorists from boarding airplanes. But in terms of the DHS role in this case, the bottom line is this: He was not on the No Fly List, which would have flagged him to be prevented from boarding; nor was he on the Selectee List, which would have flagged him for secondary screening. Furthermore, the physical screening performed by foreign authorities at airports in Nigeria and the Netherlands did not detect the explosives on his body.

Now, immediately after the attack, DHS responded. We directed the Federal Aviation Authority (FAA) to alert all 128 flights from Europe bound for the United States of the situation. We increased security measures at domestic airports. We implemented enhanced screening for all international flights coming to the United States. We reached out to State and local law enforcement, air carriers, international partners, and other relevant agencies to provide them the information they needed on the ground.

In our reports to the President, on fixing what went wrong on Christmas Day, we have also outlined five other areas of action.

First, as this incident underscores, aviation security is increasingly an international responsibility. That is why I dispatched Deputy Secretary Jane H. Lute and other top DHS officials on a multi-continent tour to meet with our international counterparts about airline and airport security. This evening, I will travel to Spain to meet with my European Union (EU) colleagues to strengthen international security measures and standards, and we will include in that information-sharing technology and other related issues.

Second, DHS has created a partnership with the Department of Energy and the National Labs to use their scientific expertise to improve screening technology at domestic airports.

Third, DHS will move forward in deploying enhanced screening technologies like advanced imaging technology and explosive trace detection machines to improve our ability to detect the kind of explosives used in the Christmas Day attack. TSA currently has 40 of the Advanced Imaging Technology (AIT) machines deployed now. We will deploy at least 450 more this year.

Fourth, we will and have strengthened the capacity of aviation law enforcement, including the Federal Air Marshal Service.

And, finally, DHS will work with our interagency partners to reevaluate and modify the way the terrorist watchlist is created, including, as mentioned, how names are added to the No Fly and Selectee Lists.

I am glad to be working with leaders like Admiral Blair and Director Leiter in addition to this Committee, who have done so much to improve our homeland security apparatus, and I am also grateful to the men and women of the Department of Homeland Security who do so much every day to guard our country against attack.

Last, I wish I could tell you, with all of this ongoing work and all of these upcoming actions, that there will never again be another Umar Farouk Abdulmutallab. I cannot do so. What I can tell you is that this Administration and the men and women of the DHS are working 110 percent every day to minimize the likelihood of a successful terrorist attack against the homeland, and I am proud to be with the Department in that work.

Thank you for the opportunity to testify, and I look forward to your questions.

Chairman LIEBERMAN. I thank the three of you for the substance and spirit of your opening statements.

I do want to indicate to my colleagues on the Committee that the three witnesses have made themselves available for a closed session with the Committee immediately following the public session if there are questions that are asked here that cannot be discussed in public session. We are going to have 7-minute rounds of questions.

Let me just go back to the post-September 11, 2001, period and to say what I think is common belief now, which is that our response at that point was to the fact that there was not information sharing going on among—there was enough information in the Federal system that we should have found and been able to stop the attacks of September 11, 2001. That is a personal conclusion. But it was not, as we used the metaphor at that time, together on the same board, so the connections could not be seen.

One of the great goals of the 9/11 Commission legislation was to make sure that, metaphorically speaking, all the information came together on the same board so it could be seen. I think what we have learned painfully now is that there is so much information that is being collected by the intelligence and other agencies of our government, it is not enough to put it on the same board. We have to create systems to find out how to connect the information that we have, either technological or human.

As you mentioned, part of what emerges from the Christmas Day bombing case is there was intelligence information about al-Qaeda in the Arabian Peninsula being involved with somebody names Umar Farouk—not the full name but the beginning of the name. His father came into the embassy in Nigeria, and said he was worried about his son, Umar Farouk Abdulmutallab. There are references from conversations picked up by the National Security Agency (NSA) from al-Qaeda in the Arabian Peninsula of a Nigerian that they were going to use for an attack. Obviously, the fa-

ther indicates a Nigerian. And somehow that did not all come together.

Now, here is what troubles me. We live in an age when any one of us and our young children, our grandchildren now in my case, can go on the computers, go to Google, and search an enormous array of databases immediately. My impression—and, Director Blair, Mr. Leiter, you respond to this—is that at NCTC we do not have that ability now. You have a series of separate databases from different parts of the intelligence community and the government, and you have access to all of them, plenty of sharing. But there is not a program, a search engine right now by which you, by act or by some automatic software programming, can have expected in this case, for instance, that there would have been a hit and an alarm on Umar Farouk Abdulmutallab, a Nigerian, December 25, 2009. Am I right? Do we not have that capacity within the NCTC?

Mr. LEITER. Senator, we do not have that exact capacity, but I would note that over the past several years we have worked with folks from across government and some of the private sector companies that you would expect have that technology.

Chairman LIEBERMAN. Right.

Mr. LEITER. And the answer uniformly has been that it is not as easy a problem as people would expect. I think we have some potential technological solutions on the very near-term horizon that we are attempting to implement within weeks. And, frankly, we were surprised, I was surprised, at the extent to which other agencies' searches were not hitting against very critical data sets that might have uncovered this, and then highlighted them for NCTC and others.

Chairman LIEBERMAN. Director Blair, do you want to add anything to that?

Mr. BLAIR. I would only amplify on what Director Leiter said, Mr. Chairman. The search tools that we now have depend on certain characteristics, and I do not want to describe them here, but they also have blind spots that do not allow the sort of Google-like idea that we have from our personal computers.

Chairman LIEBERMAN. Right.

Mr. BLAIR. Several of those shortcomings came up in this case, which we can fix. I think that the other thing that I have learned from this is that almost all of our energy was focused on building these systems, hooking together, and getting the search engines. We do not have enough of a testing regime so that we do the "what if's" before we have one of these incidents, put partial information in and see where it goes, fix those and find those for ourselves. And that sort of continued self-testing is going to be a greater part going forward so that we can make some of these mistakes for practice before we make them for real.

Chairman LIEBERMAN. So you are, with a sense of real urgency, going now after improving what I would call the search capacity across the databases you have automatically to come up with linkages. Correct?

Mr. LEITER. Correct. And I would just stress that this is not actually a new problem from our perspective.

Chairman LIEBERMAN. Right. You have been working at this.

Mr. LEITER. This is something we have been working with vehemence on. We have obviously not gotten to the point we need to get, and we are trying to accelerate that now.

Chairman LIEBERMAN. Now, the other way to deal with this, which I believe the President mentioned—or perhaps one of the reports to him did—is to assign cases, suspected cases, to people to follow. Now, that is a tough thing to do, so I would like to ask you to talk about it a little bit. In other words, presumably at some point somebody has to be concerned enough about picking a particular matter out of the thousands of cases that you add every day to your watchlist concerns. Let us take this case, that somebody would have had to say, based on the father coming into the embassy, "We have to follow this," or based on the intelligence stream that said al-Qaeda in the Arabian Peninsula was working with somebody named Umar Farouk, a Nigerian, and something was going to happen on December 25, 2009, somebody had to make that baseline decision.

But what then? Do you have the human capacity to assign people to chase these down and have a responsibility, almost as if this was a police department and you were assigning a detective to pursue a case—except, of course, here it is not to try to find the murderer, it is to try to prevent a murder from happening. So what is our capacity to deal with this with better use of personnel?

Mr. LEITER. Mr. Chairman, I think your question is exactly right. We do a very good job at hunting down the threats when we know it is a threat.

Chairman LIEBERMAN. Right.

Mr. LEITER. The more difficult thing is deciding what is a threat in the first instance and hunting it down.

There are two things that we are doing to try to improve this. Right now, I have not had the capacity to do this in the way it needs to be done because we are going to expand the scale of it, the breadth of the things that we chase down. We have been very good at chasing down those threats that come out of Afghanistan and Pakistan. We are going to be better now at chasing down those small bits of data that come out of Yemen, North Africa, or East Africa.

Two, with new resources, the plan is to establish teams that have no responsibilities other than to do that. We are calling them pursuit teams for the very reasons you identified, to find those small bits and hunt them down until we either figure out what is going on or there simply is nowhere else to go and there is no other data out there to be applied to the problem.

Chairman LIEBERMAN. Director Blair.

Mr. BLAIR. Just for context, Mr. Chairman, I would cite two things, not by way of excuses but just by way of understanding. The only conversation on resources that I had with Director Leiter in the weeks leading up to Christmas was a conversation a week before on how we were going to allocate a $30 million cut in the Office of the DNI, part of which funds the NCTC. So the general fiscal climate we are dealing with was one which was reducing resources to this.

The second thing is the pressure on No Fly Lists, as you all know, for several years before 2008 had been to make them small-

er. My cousin has a name on it and gets hassled every time. And you can tell as you read through the guidance given to analysts that they were expected to cast a very fishy eye on the inclusion of lots more names, and the pressure was in the other direction. Shame on us for giving in to that pressure. We have now greatly expanded the No Fly List from what it was on December 24, and have done a lot more of what is prudent; to put names on it just in case, and then take them off as we need to. But the pressure was quite the other direction, and as I say, I should not have given in to that pressure, but it was a factor, and we have certainly changed that attitude, and we have to maintain that over a course not just of 6 years but of 12 years and until this campaign finally ends.

Chairman LIEBERMAN. Director Blair, I cannot thank you enough for what you have just said because it seems to me that in the process for deciding what watchlists people were being put on, we were using a standard that was, as you said, legalistic. It was a legal standard. In fact, the very words, the terms being used, "reasonable suspicion," come from Supreme Court cases that govern warrantless searches by police in the United States. But we are at war with these people, and it just seems to me that if somebody brings some information to the U.S. Government that suggests in any way that a person is involved in terrorism, it at least is justification for putting them on a list that will subject them to secondary screening before they board a plane to come to the United States. It is not being used as a basis for arrest, certainly not for conviction, but this is a classic example of the ongoing tension between security and liberty. And I appreciate your admission here and your commitment to change this, that I think we were erring too much on the side of a legalistic vision of privacy or even convenience that ultimately jeopardized the security of the majority. So that is very good news, and I thank you for it.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Good intelligence is clearly critical to our ability to stop terrorist plots, and that is why I am very concerned about the decision to quickly charge Abdulmutallab in civilian court because I believe that we, by doing so, have lost an opportunity to secure additional intelligence from him, not only about his own training, but intelligence that possibly would allow us to uncover other plots that are emanating from Yemen.

We know that those interrogations can provide critical intelligence, but the protections afforded by our civil justice system as opposed to the military tribunal system can encourage terrorists to lawyer up and to stop answering questions. And, indeed, I am told that with Abdulmutallab, once he was Mirandized and received civilian lawyers, that is exactly what he did.

Mr. Leiter, were you consulted regarding the decision to file criminal charges against Abdulmutallab in civilian court?

Mr. LEITER. I was not.

Senator COLLINS. Mr. Blair, were you consulted?

Mr. BLAIR. Senator Collins, I have been a part of the deliberations which have established this high-value interrogation unit which we started as part of the Executive Order and as part of the

decision to close Guantanamo. That unit was created exactly for this purpose, to make a decision on whether a certain person who is detained should be treated as a case for Federal prosecution or for some other means. We did not invoke the High-Value Interrogation Group (HIG) in this case. We should have. Frankly, we were thinking more of overseas people, and, we did not put it in. That is what we will do now, and so we need to make those decisions more carefully. I was not consulted. The decision was made on the scene. It seemed logical to the people there. But it should have been taken using this HIG format at a higher level.[1]

INFORMATION PROVIDED BY MR. BLAIR FOR THE RECORD

My remarks today before the Senate Committee on Homeland Security and Governmental Affairs have been misconstrued. The FBI interrogated Umar Farouk Abdulmutallab when they took him into custody. They received important intelligence at that time, drawing on the FBI's expertise in interrogation that will be available in the HIG once it is fully operational.

Senator COLLINS. Madam Secretary, were you consulted?

Secretary NAPOLITANO. I was not.

Senator COLLINS. Mr. Chairman, I think that is very troubling. It appears to me that we lost an opportunity to secure some valuable intelligence information and that the process that Director Blair described should have been implemented in this case. And I think it is very troubling that it was not and that three key intelligence officials were not asked their opinion.

I would like to move to another issue that I raised in my opening statement. The facts surrounding the failure to revoke Abdulmutallab's visa really trouble me because it appears that ultimately no agency considered itself responsible for this decision. The State Department spokesman said, when asked why the State Department did not revoke the visa, "Because it is not our responsibility. It would be up to the National Counterterrorism Center to make the determination on whether to revoke a person's visa." That is not how I read the law.

Secretary Napolitano, part of the Homeland Security Act of 2002 gives DHS broad authority to set visa policy, and, in fact, it vests in the Secretary the exclusive authority to issue regulations with respect to administer, and enforce the provisions of the law relating to consular officers in connection with granting or refusal of visas, and it says the Secretary shall have the authority to review and refuse visas in accordance with the law.

So I want to get at the issue of why Abdulmutallab was allowed to keep his visa and who has the authority to look at those individuals listed on the broadest terrorist watchlist, the TIDE list, identify those who have visas, and take action to suspend those visas pending further investigation. Whose job is it? Mr. Leiter.

Mr. LEITER. Senator Collins, I will admit that when I was told of that authority that I do not have, I was surprised to learn from the State Department that they thought I did have that. And I have since spoken with Secretary Clinton, and it is quite clear that the legal authority for revoking resides within the State Department, and NCTC does not have any authority to do so.

[1] A statement for the Record provided by Mr. Blair appears in the Appendix on page 214.

To your question about have we reviewed visas against the entire Terrorist Identities Datamart Environment, we have, although the initial look was at the Terrorist Screening Center, and that number we have already reviewed, anyone who has a visa who has any information on them in TIDE and re-reviewed whether or not we should recommend to the State Department that visa be revoked.

We have also been quite aggressive in applying the no-fly criteria to individuals who have a visa, using, I would say, a less legalistic standard in applying those standards.

Finally, I do want to note that beginning in the late summer—July 2008, we began fully, in conjunction with the State Department, reviewing these applications in a way that I believe is far more advanced than that which was previously used by the State Department, and in conjunction with the State Department, NCTC now provides the State Department, Department of Homeland Security, the Federal Bureau of Investigation (FBI), and the CIA some more advanced Google-like technology to screen these visas more effectively. And I am happy to speak about that more in closed session.

Senator COLLINS. Thank you. Director Blair, whose job is it?

Mr. BLAIR. I think you are putting your finger, Senator Collins, on a characteristic of this combating terrorism effort that we need to tighten down with the strong enthusiasm for counterterrorism, the sense that we all ought to be working on it. I think we did not drive some of these responsibilities as far as we should have in terms of everybody is helping, but who is it at the end, and I think you have identified one more which we need to and are going to tighten right down so that primary, support, and ultimate responsibilities are made clearer, because there is a tendency to say, I have this new capability, let me help you, and we ought to do that. But we should not allow that to interfere with a clear understanding of who has the ultimate call.

Senator COLLINS. Thank you. Secretary Napolitano, you do have some broad authority in this area. Whose job is it from your perspective?

Secretary NAPOLITANO. Well, under Section 428, the Department has the legal authority to refuse the issuance of a visa. The State Department has retained the ultimate authority to revoke a visa once issued. But I think all of us have a role, along with the State Department, in measuring pre-existing visas against information or subsequently acquired information that comes into the system. I think that is part of the tightening that Admiral Blair just talked about.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins. Those are excellent questions. I want to make two brief points with regard to the questions you asked.

The first is to say I share Senator Collins' concern both about the decision to try Abdulmutallab in a regular Federal court as opposed to a military commission because, in my opinion, he is a prisoner of war, an enemy combatant. I am also troubled that the three of you were not asked to be involved in that decision before it occurred, and I want to say particularly as the Chairman of the Homeland Security and Governmental Affairs Committee, that I

am troubled that Secretary Napolitano was not asked to comment on that because there are obvious homeland security implications of a decision to try an accused terrorist in New York, Detroit, or Washington, DC, as we can see most practically and obviously in the recent request by Mayor Bloomberg for a first payment of $200 million for additional security required in New York around the trial of Khalid Sheikh Mohammed and the other September 11, 2001, suspects.

In fact, the Committee, Senator Collins and I are going to convene a hearing on this subject in February, the homeland security implications of the decision to try terrorist suspects in Federal courts.

The other point I want to mention very briefly—I apologize to my colleagues—is that in focusing on the visa question, I think Senator Collins has really put her finger on an important point, and we want to come back and raise a fresh question here, which is whether the visa processing responsibility really ought to be with the State Department—in other words, whether it should be with the Department of Homeland Security, and this is not really a matter of foreign policy. In some sense it may be a waste of the time of Foreign Service officers to have them interviewing people to decide whether they are eligible for a visa or not. It really is much more a question of the law and homeland security, whether it is in terms of the legitimacy of immigration or the threat of terrorism. So we are going to come back and do a separate hearing on that as part of this oversight. I am not inviting a response unless you wish one. As a matter of fact, I am going to ask you to hold it until my time because I do not want to intrude on my colleagues' time.

I will call Senators in order of arrival, as is our custom. That would be Senators Tester, McCain, Burris, Ensign, Bennett, and Pryor. Senator Tester.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Thank you, Mr. Chairman. I want to thank Director Leiter, Admiral Blair, and Secretary Napolitano for being here today.

There have been some reports coming out of Canada that suggest an increasing concern about radicalization of some Canadians with ties to the Middle East and the possibility of Canada becoming a stopover point for terrorists who try to enter the United States.

What do you think about these assessments? How seriously should we take these reports? Canadian Television (CTV) reported regarding the efforts to actually bringing trained terrorists into the United States through Canada. Could you tell me what you think of that potential threat and potentially what we are doing about it?

Secretary NAPOLITANO. Senator Tester, I think the answer to that question should be discussed in the closed part of this meeting.

Senator TESTER. That would be fine.

Secretary NAPOLITANO. I will say, however, that we have had extensive personal discussions with law enforcement and security officials in Canada, not just in the wake of December 25, 2009, but also in preparation for the Olympics that will be held there.

Senator TESTER. And no problem, we can do that in closed session. You feel the same way. OK, that will be good.

Our borders are only as strong as the weakest link, and we do not want a panic and shut down of the border because we have trade issues and we need to have a balance there. But when folks can come into the country with explosives sewn into their clothes, as happened on Christmas Day, it means that we have issues not only in our airports but also our ports, and it means that the issues that you folks talked about in your opening statements are critically important.

I want to talk about the technology portion of this. Secretary Napolitano, you talked about this being an international situation as far as the screening goes. Director Leiter and Admiral Blair deal with the issues before they get to the point where they walk in the airport, and if that information is sorted through correctly and went through the sieves right, we can catch them before they even go through the screening.

Is the screening adequate in other countries to be able to even catch—I mean, Admiral Blair talked about the fact that these explosives were known about, this type of explosive. Is the screening inadequate to catch the technologies that are coming down the pike, even when we know about them?

Secretary NAPOLITANO. Senator Tester, I think the point is that there are multiple layers of security that need to happen, no single one of which is a 100-percent guarantee or a silver bullet. The layers, when they act properly, increase the likelihood that you will prevent something from happening.

Once you get to the airport domestically, that includes explosive detection machines; it includes the advanced imaging technology; it includes law enforcement; and it includes dogs. Now, internationally, it is different. We do not control in that sense international airports or screening procedures. Indeed, we do not even do the screening ourselves. What we do is if we have somebody on the Terrorist Screening Database list, it is advised that additional screening should be done.

What we are doing now is embarking on a very aggressive international effort using this incident as the catalyst for all countries, all of whom have passengers who fly, to lift their overall screening and airport procedures because indeed there is great variation around the world.

Senator TESTER. OK. So what you are saying is at this point in time—and we are talking generally here—the screening that goes on in foreign countries is not as adequate as the ones that go on here domestically.

Secretary NAPOLITANO. It depends on which airport you are talking about. For example, let us use Schipol, the airport in Amsterdam. The screening there is not dissimilar from the screening in the United States, and the screening that Abdulmutallab went through is not dissimilar from what he would go through in many of the airports in the United States. What we have added and are adding domestically are more canines, and more explosive detections, more advanced imaging technology.

Now, airports in other countries or other countries have resisted using some of those items because of other concerns that they have,

about privacy, for example. This incident, however, like I said, is serving as a catalyst to reopen that dialogue, particularly with the airports in countries where we have a large throughput of passengers to the United States.

Senator TESTER. I want to come back to that, and I am assuming there will be another round of questions. We are going to shift totally off of this just for a second while I have you here.

We all know what has happened in Haiti over the last 7 to 10 days. It has been devastating, and that is an understatement. There is an issue about adoption of potential Haiti children who have been left without their parents. We have about five families right now that have completed all the paperwork to get the children from Haiti. And yet they are being held up. I need to get a commitment from you that the Citizenship and Immigration Services, an agency within your Department, will work with my office to help expedite our ability to get those kids out. As you can imagine, the constituency is very anxious. It is a terrible situation. I just need your help in making this work.

Secretary NAPOLITANO. Senator, you have that commitment, but may I give a longer answer to that?

Senator TESTER. Sure.

Secretary NAPOLITANO. Because I think the public needs an understanding of this.

Senator TESTER. Yes, absolutely.

Secretary NAPOLITANO. And this actually has been one of the—the DHS can work at so many levels on so many things, so the Coast Guard has been in Haiti. The Federal Emergency Management Agency (FEMA) has been helping U.S. Agency for International Development (USAID) get help into Haiti. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) have been providing assistance. The issue of orphans is one that is tragic, and I think as we go forward and begin to learn the amount or the number of casualties, it is going to grow.

Senator TESTER. Yes.

Secretary NAPOLITANO. It is something that needs to be handled very carefully because there are many issues involved in terms of making sure that people—I am not going to say these five children, but other children that come to us are indeed orphans until all the search and rescue is done or other families are located.

There are other issues involved as to whether the adoptive parents in the United States are qualified for adoption under the applicable law.

There are issues about the health and welfare of the children when they are brought to the United States. Many of them need to be immediately put into the care of the Department of Health and Human Services (HHS) and checked over thoroughly before they can be moved.

So we have formed a team—it is the State Department, it is us, it is HHS, as three of the big components, to really work on this adoption issue because we all want the right things for these children. This issue is only going to grow over time.

Senator TESTER. That is correct, and I appreciate the opportunity to work with you and your group of people on this issue. And I

thank the Chairman's indulgence for pulling off topic for a moment. We will be back. Thank you very much.

Chairman LIEBERMAN. Thank you very much for your questions, and particularly the last one, Senator Tester. We are all sharing your concern.

Next is Senator Burris. Good morning.

OPENING STATEMENT OF SENATOR BURRIS

Senator BURRIS. Thank you, Mr. Chairman. Happy New Year to everyone. I was just going to say that it is crucial to recognize the contribution of Office of the DNI, NCTC, and DHS for making our homeland as secure as it is. So you all are to be complimented for the work that you have done. And there have been numerous terrorist plots foiled since September 11, 2001, some of which have occurred in my home State of Illinois. So we are very grateful to you all for that effort.

And I just wonder, is there a resource problem here? Mr. Leiter or Mr. Blair, is there a resource problem?

Mr. LEITER. Senator, first of all, thank you for your kind words. The kind words we really want are just the thank you's when we keep doing things right, so I appreciate the kind words now. But this is not an occasion that we are happy about in any way.

Resources have been an issue. As Director Blair said, we were facing cuts at the end of last year. Thankfully, with the Director's help, those have been avoided. And in order to do some of the enhancement of the watchlists so we make sure that when you have an Umar Farouk, you put that together with Umar Farouk Abdulmutallab and all the information, and you have teams that can pursue the small bits of information rather than just the high-profile threats, it does take more resources. And Director Blair has been extremely supportive of that, as has been the White House.

Mr. BLAIR. Senator, we have moved money and people in the near term to put more on helping NCTC, and there will probably have to be some adjustments in the overall budgets in order to sustain that.

Senator BURRIS. I just wonder, in our democracy, as I was watching the news on this issue of that Detroit bomber and watched it on Media Report, I just had some concern about what was being reported for future actions. And I do not know whether or not this can come up in a closed hearing or not, but I was concerned when the media was reporting where the airports are that we are now going to be screening from. So the simple response is, OK, if I am a terrorist, what am I going to do? I am not going to be bothered with it. There is some information that we have to keep classified in terms of where the international screening is going to come from and will not be knowledgeable to the general public. Americans demand our right to know, but there are some things that are not going to make us safe if we know them and everybody else knows them.

Mr. BLAIR. I could not agree more, Senator Burris, that the public discussion of the specifics of the defensive measures we take are making it that much easier for people to evade our defenses and come in. The kind of hearings that we are having this morning where you have responsible witnesses who think through what

could be unclassified and what is classified I think are absolutely essential for the functioning of the democracy. The unauthorized leaks of the NSA intercepted this or a CIA human report said this or this airport is good, I think, is just making the job of those who are working hard to try to defend us that much harder. It costs the taxpayer that much more money, and I wish people would just shut up. [Laughter.]

Senator BURRIS. It makes sense to me because that was my immediate reaction when I see this list reported on television of what airports we are now going to be putting in special screeners.

Which leads to another question that might not be answered here, and I probably will not be able to attend the closed session because I have to preside very shortly. But I am concerned about the possibility and the techniques that are now being used by the terrorists. I mean, I did see a movie just recently coming back from China. There was a movie on the plane, Mr. Chairman, and the movie was "The Traitor." I do not know if anyone has seen that movie. It is really about the terrorists and how they were going to set bombs here in America. And I just hope that we are anticipating all the various processes. One time it was a shoe. This time it was underpants. What will it be the next time? And I am pretty sure you all cannot disclose this at this point, but please disclose this for the record in our closed hearing. What are some of the techniques that you all are assessing that would try to be on the offensive, as you said, Director Blair? You have to be on the offense and the defense, but we have to be on the offense in these regards. And I am sure that you are, but I just want to re-emphasize that, because I can say for the record I think about the small towns across America. If I were a terrorist, I would not go after Chicago, I would not go after New York. You know where I would go? I would go to my hometown of Centralia, Illinois, where there are 14,000 people, and raise havoc in there which would scare Americans to death.

So, Madam Secretary, we have to be concerned about homeland security as we look at our small communities and the resources that they would have in case of being struck by a terrorist. Is there a comment there, please?

Secretary NAPOLITANO. Senator, yes. One of the criticisms that we have talked about amongst ourselves is being reactive as opposed to proactive all the time. Well, of course, you have to react and fix what went wrong. Once you have identified a problem, you have to fix it. But we also need to be thinking ahead to be proactive.

That is why, for example, we have entered into this agreement to really get some of the best scientists in the world who are in our National Labs thinking well ahead about the next generation of screening technology and what it can show us.

The other thing is that the threat is constantly evolving, Senator. When I came into office, I was receiving very little information about American or U.S. citizens that were themselves radicalized to the point of terrorism. That has changed over the course of the year. Director Leiter has already talked about the emergent threat out of Yemen. So there is a constantly evolving environment that we have to deal with and be thinking ahead.

So the challenge for us—and it is a challenge for us at this table, it is a challenge for others, it is a challenge for the Congress, it is a challenge for our international partners—is to always be thinking about the next iteration that is being conceived.

Senator BURRIS. Mr. Chairman, just one quick point, and I would like to comment on something that Ranking Member Collins made in reference to where this person would be tried. And I understand that intelligence was gathered from this person prior to him being given his rights. So I do not know whether or not that could be disclosed in a closed hearing as well to alleviate some of the anxiety in reference to whether or not we were able to get any information from this young man, which I understand there was substantial information acquired prior to Miranda.

Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Burris. Senator McCain.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Well, thank you, Mr. Chairman. I thank the witnesses, and I thank them for their continued service to the country.

I think everybody knows the facts of the Christmas Day bomber. A person buys a ticket with cash, a one-way ticket. His father has already warned the CIA. The series of missteps that have taken place led to this near tragedy. And I thank the witnesses for their candor and being forthcoming about these failures.

The President said, on January 7, "I repeatedly made it clear in public with the American people and in private with my national security team that I will hold my staff, our agencies, and the people in them accountable when they fail to perform their responsibilities at the highest level."

I would like to ask all three witnesses who has been held accountable. I will begin with you, Mr. Leiter. Has anybody been fired? Has anybody been transferred? Has anybody received a letter of admonition? Has anybody been put on leave?

Mr. LEITER. Senator, we are, in fact, conducting internal reviews to determine whether or not any of those should be pursued.

Senator MCCAIN. And how long will those reviews take? It is fairly clear the facts of what happened. Isn't it?

Mr. LEITER. Well, actually, I think many of the facts are clear. I would correct the record on a couple of points.

In fact, the fact is not that he bought a one-way ticket. He bought a round-trip ticket.

The fact that he used cash, frankly, in Africa is completely and utterly——

Senator MCCAIN. That was in Copenhagen, not Africa.

Mr. LEITER. No, sir. I believe he bought that——

Senator MCCAIN. Did he have someone who facilitated his—if you are defending——

Mr. LEITER. No, sir.

Senator MCCAIN. That we should not have found—should not have been alerted to this individual, sir, then——

Mr. LEITER. Senator, I apologize. I do not want to——

Senator MCCAIN. All right. Has anybody been held accountable?

Mr. LEITER. We are reviewing all the individuals, and I think the President is reviewing my performance as well. That is absolutely appropriate.

Senator MCCAIN. Admiral Blair.

Mr. BLAIR. You and I have a Navy background, Senator McCain, and you know that you do two investigations when something bad happens. The first is a safety investigation to fix the parts of the system so that you get the word out and ensure it does not happen again. The second is the accountability part of the investigation——

Senator MCCAIN. Actually, it has been my experience, Admiral, that when the captain of the ship does something wrong, or something goes wrong on his watch, the captain is relieved immediately. You can go all the way back to the *USS Missouri,* sir.

Mr. BLAIR. The captain is sometimes relieved, and sometimes he is not. It depends what happened in the cases.

Senator MCCAIN. The captain is relieved until such time as he is cleared. So I will be glad to go over naval history with you. Has anybody been held accountable?

Mr. BLAIR. We are doing the investigations now so that we do not hold people accountable based on bad information but we do hold them accountable based on what actually occurred and what the standards that they were expected to perform to were. And that is underway.

As I said in my opening statement, the system was capable of doing this. All the pieces did not operate the way they should. I personally have a large degree of responsibility for making sure those pieces are working, and we are working to make that happen. I do not feel good about it, and I am fixing it.

Senator MCCAIN. I was not asking whether you are fixing it or not, Admiral Blair. So far, it has been several weeks, and no one has been held accountable. Secretary Napolitano.

Secretary NAPOLITANO. Well, as you know, Senator, we do not prepare the No Fly or terrorist list, and we do not do the screening at international airports. However, I am the Secretary of Homeland Security, and I think I share responsibility for the enterprise that has to happen to prevent this from happening again.

Senator MCCAIN. I thank you, Madam Secretary.

I understand, Director Blair, in response to Senator Collins, that you were not consulted as to what venue the Christmas Day bomber would be tried in. Is that correct?

Mr. BLAIR. That is correct. Yes, sir.

Senator MCCAIN. How about you, Mr. Leiter?

Mr. LEITER. No, I was not.

Senator MCCAIN. Secretary Napolitano.

Secretary NAPOLITANO. No.

Senator MCCAIN. So I guess I have to ask your opinion, Admiral Blair. Should the Christmas Day bomber be tried in civilian court, or should it be under military tribunal? Since they would not ask you, maybe I should.

Mr. BLAIR. I am not ready to offer an opinion on that in open session. We can talk about it in closed session, Senator McCain.

Senator MCCAIN. Mr. Leiter.

Mr. LEITER. Senator, I honestly do not have a position. I have been fully engaged in trying to fix this, and I have not focused on where he would be charged.

Senator MCCAIN. Well, unclassified information indicates that the Christmas Day bomber was providing information that was necessary to try to crack this case, and when he got a lawyer, he immediately stopped that information. Now, that is according to public documents. I do not have any classified information. If that is the case, I think it is a terrible mistake. I think it is a terrible, terrible mistake, when it is pretty clear that this individual did not act alone.

Admiral Blair, in your testimony before the Committee, you stated you would exercise your authorities to the fullest and withhold judgment on whether the Intelligence Reform Act provided the DNI with sufficient authority. Now, can you share with the Committee whether you believe the DNI has sufficient authority to manage intelligence issues that affect America's public safety?

Mr. BLAIR. Senator McCain, as this job continues—it has been 5 years now since the Director of National Intelligence was established—I find that you discover new things that you have to fix as you go along, and this incident is exposing some of those.

The authorities of the DNI I think heretofore were able to make the big pieces happen. There was lots of sharing of information in this case, but we are finding now some individual pieces in which I think more authority may be required. So the overall answer to the question is I do not know quite yet, but the authorities granted heretofore by the Congress have been adequate to make important improvements happen.

Senator MCCAIN. I thank you, Mr. Chairman. I thank the witnesses.

Mr. Chairman, I do find it interesting that apparently none of the three top individuals were consulted on a decision whether to put the Christmas Day bomber into civilian court or military tribunal, and I think whoever advised them of that—and I think this decision was a terrible mistake which could impact our ability to defend this Nation.

I thank the witnesses.

Chairman LIEBERMAN. Thanks, Senator McCain. Senator Ensign.

OPENING STATEMENT OF SENATOR ENSIGN

Senator ENSIGN. Thank you, Mr. Chairman.

Admiral Blair, you said that this HIG was not convened. Who made the decision—since none of you were consulted, who made the decision to go ahead and Mirandize the prisoner?

Mr. BLAIR. It was a decision made by the FBI team, the agent in charge on the scene consulting with his headquarters and Department of Justice.

Senator ENSIGN. Who authorized him at the Department of Justice? How high up did this go?

Mr. BLAIR. I do not know, sir.

Senator ENSIGN. Do any of the rest of you know?

Mr. LEITER. I do not know, Senator.

Senator ENSIGN. Secretary Napolitano, you talked, in response to Senator Collins' question, about you have some responsibility, you

have some authority to deal with the visas, and we understand that the State Department, I guess, Director Leiter, you talked about you did not know you had the authority—or did not have the authority.

Mr. LEITER. I do not have the authority.

Senator ENSIGN. Has there not been a case in the past where somebody brought to you rather, have we not rejected any visas?

Mr. LEITER. The State Department has the authority to revoke the visas.

Senator ENSIGN. I understand that. Has any one in your organization before brought you a case where you thought that there should be a visa rejected where you actually found out that you did not have that authority before the Christmas Day bomber?

Mr. LEITER. We routinely provide intelligence to the State Department to make that decision.

Senator ENSIGN. That is not an answer to my question. In other words, somebody who is within your organization, they had information, this person should be rejected, did you not then make a recommendation and find out you did not have the authority? Or has anybody brought that information to you before?

Mr. LEITER. Senator, I think the spokesperson for the State Department was simply confused, and no one in the State Department who works these issues actually thought that I had the authority to revoke a visa, because we do not.

Senator ENSIGN. That is not what I am saying. Try to understand my question.

Mr. LEITER. I apologize, Senator.

Senator ENSIGN. Has somebody in your organization before brought you information about somebody who should be rejected?

Mr. LEITER. The answer is no because no one in my organization believes that I have the authority to reject visas.

Senator ENSIGN. So they know that already.

Mr. LEITER. Yes.

Senator ENSIGN. You just did not know it, but everybody in your organization knows——

Mr. LEITER. I apologize, Senator. My attempt at humor was clearly lost. I joked with Secretary Clinton I did not realize that I had the authority, because clearly I did not ever have it. It was only the State Department's spokesman that was confused about where that authority lay.

Senator ENSIGN. Secretary Napolitano, getting back to my question about Senator Collins—and this has been brought up, like who is responsible for this colossal failure. In business, you understand that if there is not one person responsible for making certain decisions, like if there are several people, then no one can be held accountable, and no one makes the decision. It has to do with whether it is the visa rejection or whatever. It gets back to what Senator McCain was talking about, if no one really feels that they are accountable, the decisions are not made and people really do not know who is supposed to make the decision.

Is that being addressed in this whole evaluation process of what went on?

Secretary NAPOLITANO. Senator, yes, in a variety of ways, but I think Admiral Blair explained in his opening statement that one

of the things that is being addressed is who has the responsibility to follow up on different lines of intelligence as they come in.

Senator ENSIGN. And so are we going to have a clear set of guidelines and know that this person is responsible for making that decision. Is everybody going to know what they are supposed to do and what they are not supposed to do in the future, I guess is the best way to ask? And when will we have all those procedures in place to where everybody knows what they are supposed to and not supposed to do?

Mr. BLAIR. We have a 30-day deadline that the President established to provide authoritative proposed pieces of paper that could be anything from an Executive order down to an intelligence community directive, which I would sign, or similar authorities within Secretary Napolitano's organization. So it will be quite clear as to who has responsibility for what. We agree that has been loose.

Senator ENSIGN. As part of that, you mentioned the HIG that was not convened, and you said in the future that absolutely will be convened.

Mr. BLAIR. Yes, sir.

Senator ENSIGN. In any case like this, that is a guarantee from you. That is a guarantee from this Administration that is not going to happen in the future; this will be convened.

Now, from what I understand, even with the HIG, though, you will only use intelligence techniques that are approved under the Army Field Manual. Is that correct?

Mr. BLAIR. The type of interrogation techniques will be calculated by the purposes for which we want to make that information available, whether it be law enforcement or for intelligence. If it is intelligence, then, yes, the techniques that are in the Army Field Manual will be used by the interrogators.

Senator ENSIGN. And the Army Field Manual is public, correct?

Mr. BLAIR. That is correct.

Senator ENSIGN. This Administration stopped using any kind of classified techniques so that terrorists basically can train to the interrogation techniques that are in the Army Field Manual since they are public. But if we use classified ones, in other words, keeping the terrorists kind of guessing what they were going to be going through, it would be harder to train. Wouldn't you agree?

Mr. BLAIR. The experience we have so far is that the amount of information that we get from somebody depends on the skill of the interrogators, and we will have the very best interrogators on this HIG unit.

Senator ENSIGN. That does not answer my question. The terrorists are allowed to train to the techniques in the Army Field Manual, which is a public document. Correct?

Mr. BLAIR. The terrorists know what the techniques are, but as I said——

Senator ENSIGN. Right. But if they were classified—in other words, what the intelligence community used to use as far as classified techniques—it is much harder to train to those. Wouldn't you agree?

Mr. BLAIR. I do not think it would make a decisive difference, no.

Senator ENSIGN. You do not think that we get better information? Why do you think the intelligence community used classified

techniques before, then, where they thought it was better? Why do you think that throughout our intelligence community they used those kind of techniques before if they did not feel it was superior to the techniques used with the Army Field Manual?

Mr. BLAIR. We have looked at that quite carefully, Senator, and we do not know whether that same information that was gained through enhanced interrogation measures could have been obtained without them.

Senator ENSIGN. I guess that is something we will have to disagree on.

I want to get to one last point, because you made this comment that I thought was pretty stunning, that whoever it was was more concerned about what folks were thinking overseas. You even used the word "duh" when you were talking about whether or not to try this person in civilian court and to Mirandize this person. Can you further explain what you were talking about, the Administration being more concerned with folks who were overseas and what their opinion of folks overseas was?

Mr. BLAIR. That was not the context in which I made the remark, Senator?

Senator ENSIGN. Can you further explain what you were talking about?

Mr. BLAIR. It had to do with our being able to pursue both the threat to the United States coming out of Yemen and being able to pursue violent extremist activities or terrorist threats within Yemen itself. We needed to be able to do both at the same time.

Senator ENSIGN. Yes, this was in response to whether or not he was going to be tried in civilian courts, and that is when you said we were more concerned about what they thought overseas.

Mr. BLAIR. Let me think back to that, right. I said that when we put the HIG together, the main use for it we were thinking of was when terrorists were captured overseas, and we did not think about that case in which a terrorist was apprehended, as this one was, in the United States, and we should have thought of that. We should have automatically deployed the HIG. We will now. We will make a new mistake. We will not make that one.

Senator ENSIGN. Thank you. Thanks for clarifying that.

Chairman LIEBERMAN. Thanks, Senator Ensign. I was going to suggest that we could run the search engine on the transcript of the hearing for the word "duh." [Laughter.]

We could find that.

Mr. BLAIR. We have a search engine that can do that.

Chairman LIEBERMAN. Thanks, Director Blair.

Senator Coburn is next, to be followed, if they are present, by Senators Carper, Akaka, and Levin. Senator Coburn.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Thank you. I thank each of you for your service. You have a tough job, and when things go wrong, it is our job to help you figure out how to get it right. I think all of you are dedicated to fixing the problems.

I have worked with my Intelligence Committee staff to make sure that I stay within the bounds of what we can ask in here. I was going to attend the closed hearing, but I will wait until our

Thursday meeting in the Intelligence Committee. I have a couple of questions for both Director Blair and Director Leiter.

The intelligence community has been largely consistent in noting that had all the pieces of intelligence been connected, this individual would have met the criteria for the watchlist. However, there have been inconsistencies in views regarding whether he would have been put on the No Fly or Selectee Lists. You stated in your testimony that it would have been determined by the strength of the analytic judgment, but officials in your organization have said he would not have met the criteria for no-fly or selectee, and that is what they have reported to me.

Can you explain the criteria in whether or not the information would have risen to the level of no-fly or selectee?

Mr. LEITER. Senator, it is not an easy yes-no question.

Senator COBURN. I understand that. That is why I have asked you to explain it.

Mr. LEITER. Where he would have been placed, Selectee or No Fly List, really would have depended on what the analytic judgment was at the time. So looking at the signals intelligence and looking at what the father said, you put that together. Would the analyst have said we have a potential al-Qaeda in the Arabian Peninsula operative, or we have a potential al-Qaeda in the Arabian Peninsula operative who may be boarding an airplane to use a suicide bomb, or this individual is involved in plotting around December 25, 2009, to attack the United States?

On that first one, under the existing standards, I think he is likely on the Selectee List but likely not the No Fly List. On the later analytic judgments, it is more likely that he gets into the no-fly criteria.

It is easy after the fact to look back and say clearly he should have been on the no-fly, but it really would have depended on what the analysts said, putting all those pieces together about what kind of operative he was and what his intention was.

I think from my perspective the right answer, Senator, is we should not try to parse it so closely in the first instance.

Senator COBURN. I agree.

Mr. LEITER. We ought to have standards that allow, frankly, a greater degree of flexibility that you do not have to be able to predict exactly when the individual is going to do. If he has certain associations and is involved in any sort of operational activity, it is a pretty clear answer, and that should be no-fly.

Senator COBURN. Right. So we ought to err on the side of caution.

Mr. LEITER. I think that is certainly my——

Senator COBURN. Is it not true that there was a lot of political pressure because of so many people on the No Fly List and duplicative names that we actually reassessed that in the recent past and made it harder to put people on that list?

Mr. LEITER. That is absolutely correct, Senator.

Senator COBURN. Director Leiter, in your testimony today, you said that Mr. Abdulmutallab was identified as a known or suspected terrorist and he was entered into the TIDE list. You went on to say that the derogatory information associated with him did

not meet the existing policy standards for him to be watchlisted, let alone be placed on the No Fly or Selectee List.

Can you explain how someone who you have said was identified as a known or suspected terrorist and about whom you have required biographic data does not meet the criteria for him to be watchlisted?

Mr. LEITER. Yes, Senator, and I want to make clear at the beginning, we made a mistake in not associating all that information with him.

Senator COBURN. Right.

Mr. LEITER. And, obviously, at that point he would have been in the Terrorist Screening Database and on the watchlist. We have a not insignificant number, roughly 100,000 individuals, who have some association with terrorist groups. They may be family members or the like, or they may have lower levels of derogatory information. That standard is simply lower than what was adopted in August 2008 and promulgated in 2009 for inclusion in the official watchlist. So it was simply a matter of the data that we associated with him not meeting that higher standard.

Senator COBURN. All right. Secretary Napolitano, thank you for your service. I am pretty concerned with a couple of things that are going on at TSA, and I would refer you to an article by Mr. Litwack yesterday in the *Wall Street Journal* about body scanners. I do not know if you have seen it.

Secretary NAPOLITANO. I have not.

Senator COBURN. I would recommend it to you.

The other thing that I wanted to raise with you which gives me great pause is the fact that when the inspector general (IG) looks at what TSA is doing in terms of screening techniques, in terms of the equipment, what we have is a failure to meet your own standards as we install equipment. I would caution—and I will have this conversation with you privately based on the information we have looked at and gleaned from IG reports and also experience that we have seen—that as we respond to the public outcry for us to do more, the potential to waste a ton of money on something that is not going to be qualified to actually change the outcomes of this past December 25, 2009. I would just raise with you that I am highly concerned about that.

As a medical doctor, I am highly concerned about the exposure we are going to expose people to. I also am highly concerned that the technology we have today would not have stopped this even if we had had full-body scanners in use—in fact, we would not have. I would love your comments on that.

Secretary NAPOLITANO. Right. Without commenting on a *Wall Street Journal* article that I did not read yesterday, I can say with respect both to a Government Accountability Office (GAO) and an IG report on the scanners that they were looking at a limited sample of an earlier iteration of the technology. The technology has clearly evolved rapidly over time, but we are continuing to push the technology. That is why we have asked not just our Department but the Department of Energy and the National Labs to get involved.

From the objective evidence, the scanners that are being deployed now clearly give us a better chance of picking up be it met-

als, non-metals, powders, or liquids that somebody may be trying to get onto a plane.

Senator COBURN. Externally?

Secretary NAPOLITANO. We can talk in a classified setting about that, sir.

Senator COBURN. What I will do then is, based on the analysis of my staff on the operational testing of your screening technologies, I will send you follow-up questions, if I may, and if you would get those back to me fairly soon, I would appreciate it.

Secretary NAPOLITANO. We would be happy to do so.

Senator COBURN. Thank you. And thank you again for your service.

Chairman LIEBERMAN. Thank you very much, Senator Coburn.

Senator Carper had to leave for a moment. Senator Akaka, you are next.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, for having this hearing, and I want to add my welcome to the witnesses who are here.

I have been concerned about privacy and civil liberties in all of this. As President Obama has made clear, weaknesses in our counterterrorism systems and human errors have created gaps in our Nation's defenses. It is vitally important that we address these gaps, of course, quickly. However, we should not sacrifice our principles nor undermine our long-term strategic efforts against al-Qaeda and other terrorists. So I would like to make two points.

First, Congress, working closely with the Administration, must protect privacy rights and civil liberties while trying to improve our Nation's defenses.

Second, we should be mindful that passenger screening technologies, better databases, and different procedures alone cannot ensure the safety of our flying public. I believe that we should enhance our international partnerships, use imagination and risk-based thinking in exploring potential threats, and give our security workforce the range of tools, training, and support it needs to protect the American people.

Secretary Napolitano, you are tasked with quickly increasing the use of technology in air passenger screening consistent with privacy and civil liberties. How involved will DHS' Privacy and Civil Liberties Offices be as new technology such as whole-body imaging is deployed more widely?

Secretary NAPOLITANO. They are involved, Senator, right now and have been involved from the beginning in terms of how we deal with privacy and some of the objections raised particularly with respect to the advanced imaging technologies. I would iterate the face is screened, the person reading the image is not at the place where the screening is done, so there is a great deal of privacy in that regard with respect to an individual identity already built into the system. But even as we move forward, we have our Office of Privacy and the Office of Civil Rights and Liberties engaged in the process and the decisionmaking.

Senator AKAKA. Director Blair and Director Leiter, the Corrective Action Statement also requires your organizations to improve tech-

nology related to intelligence and to enhance watchlisting capabilities. Unfortunately, the Privacy and Civil Liberties Oversight Board, which was created by the Intelligence Reform Act to protect Americans' privacy and civil liberties, has not been set up.

How will your agencies ensure that corrective actions in response to the Christmas Day plot take privacy and civil liberties into account?

Mr. BLAIR. Senator, let me say that I think that panel should be manned up and started. It would provide a very valuable service. We do have our civil liberties and privacy officer very much involved as we consider the changes that I described in my testimony.

But I would take your question one other direction, and that has to do with families and the personal effect of what we are talking about. We have been pretty much about talking standards, regulations, screening, and so on. The Chairman introduced me to members of the families of some of the September 11, 2001, victims before this hearing, which reminds us there are real people involved in this stuff, not just big bureaucracies.

I am also reminded that it was a father who came into the embassy in Abuja and talked about his son that he was worried about who had gone to Yemen and was potentially falling under radical influence.

We know that last fall there were five young men from Northern Virginia who went to Pakistan, and it was their parents, their families who came in and told authorities about them so that they could be identified.

And while we talk about all of the responsibility of government and everything we are doing at the bureaucratic level, I think concerned, aroused citizens, families, are an absolutely key part of keeping ourselves safe and, that we should not either underrate or neglect this, and that it is a very proper emphasis. And so when we are dealing with families, we need both to rely on their help and to make sure we are not violating their civil liberties that they expect as Americans.

Senator AKAKA. Director Leiter.

Mr. LEITER. Senator, I fully agree with the view that we have to have civil liberties as a central tenet in all of this. In the Director's Review Panel that he set up, it includes four individuals, one of whom is the civil liberties protection officer. We have had the civil liberties protection officer review the watchlisting changes we have made. The one thing I would note, though, is it is very easy for me to recommend to Secretary Napolitano to put everyone on the watchlist or on the No Fly List. There are enormous and I think unacceptable costs to doing that. So what we need to have is an agreement among the Executive Branch and Members of Congress about what the proper balance is because there is a balance that was struck prior to December 25, 2009, and I think, frankly, we are now being told that a different balance should be struck.

So I am very eager to engage in that discussion with this Committee and other committees to make sure we hit the right balance because I do not want to be here after the fact again saying, well, if only we could have done this.

Senator AKAKA. Director Blair and Director Leiter, according to the 2009 Information Sharing Environment Report to Congress, DNI and NCTC had not completed their Information Sharing Environment privacy protection policies. DHS has developed its policy.

What is the status of DNI and NCTC developing their policies?

Mr. BLAIR. Senator, I am not sure exactly what policy that refers to. I will have to check and get back to you. But we are very vigilant about getting those policies out, so let me find out where the shortcoming is that was referred to in that report.

Senator AKAKA. Thank you. Director Leiter.

Mr. LEITER. Senator, I believe it is actually one consolidated policy. We are working on that, and we will supply that for the record. And, clearly, especially in light of these events, that has to be completed so you understand what the rules are we are applying.[1]

Senator AKAKA. Thank you so much for your responses. Mr. Chairman, thank you.

Chairman LIEBERMAN. Thank you, Senator Akaka. Senator Levin, welcome.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you very much, Mr. Chairman, and I add my welcome to our witnesses.

Apparently, somebody at DHS flagged Mr. Abdulmutallab for extra immigration screening while the plane was in flight. Is that correct?

Secretary NAPOLITANO. Yes.

Senator LEVIN. What triggered that?

Secretary NAPOLITANO. Let me, if I might, Senator, explain the process. Customs and Border Protection, when it gets the passenger list, pushes out to the immigration group known as the Immigration Advisory Program (IAP) in a foreign airport anybody that appears on the terrorist watchlist or the No Fly List. The No Fly List is a list given to the carrier, and basically it says do not put this guy on a plane. The terrorist list says to a foreign airport, a foreign government, you should put this person into more secondary screening, whatever that happens to be.

Now, there is other information that Customs has that involves whether that person should be questioned before they are admitted into the United States. It is the difference between whether they should be allowed on a plane, which is really a TSA, a national, a different standard than——

Senator LEVIN. This was an automatic process.

Secretary NAPOLITANO. Yes. Versus is there other information that should be explored when they are here, before they are actually admitted into the United States.

Senator LEVIN. I understand. This was a regular routine process that——

Secretary NAPOLITANO. It was a regular routine process, and based on the regular routine process at that time, the information on the text list that would have led to the State Department note was something that they would have pursued when he got to Detroit.

[1] The document submitted by Mr. Leiter and Mr. Blair appears in the Appendix on page 215.

Senator LEVIN. Right. Now, your DHS agent in Amsterdam, did he have access to that same information?

Secretary NAPOLITANO. No. He has access to the No Fly and the terrorist watchlist.

Senator LEVIN. But should he not have access to the TIDE list? Your DHS agents in seven cities, or whatever the number is——

Secretary NAPOLITANO. It is nine. Yes, nine airports.

Senator LEVIN. Should they not have access to the TIDE list?

Secretary NAPOLITANO. Senator, let me, if I might, take that in two parts.

One, with respect to that particular portion of a State Department list that listed him—it is known as the P3B—we have changed that in light of December 25, 2009, to push that forward like we do the terrorist watchlist, like we do the No Fly List.

Senator LEVIN. So would your agent in Amsterdam——

Secretary NAPOLITANO. But the entire TIDE list, the entire TIDE list includes people who, were previously accused of bringing in the wrong type of ham across the U.S.-Mexican border. It is a huge list. And the question or the understanding we need to have with the Congress is, where is Customs done, where is admissibility, where are all those types of questions done. The staff, the resources, etc., for those questions is domestic.

Senator LEVIN. The information that was pushed forward to your immigration folks here in this case now is being pushed forward to your DHS agents in other cities. Is that what you are saying?

Secretary NAPOLITANO. Yes, sir.

Senator LEVIN. So that this man would have been subject to extra inquiry in Amsterdam if the current system had been in place then?

Secretary NAPOLITANO. Yes, sir.

Senator LEVIN. OK. Now, Great Britain did not apparently allow this man to have a visa. Do we share information with Great Britain or other EU countries as to who is on their lists?

Secretary NAPOLITANO. We share some, but that is one of the reasons that we have embarked on an international effort because that information sharing needs to be tighter more than it is, more real-time than it is, and more complete than it is in the air environment.

Mr. LEITER. And, Senator, if I may, just to clarify, he was denied his visa for non-terrorist reasons, and the British did not share—and I have spoken with my British counterparts—did not have information that he was associated with terrorism other than that which we have talked about in the signals intelligence——

Senator LEVIN. Other than that, though, we are now working out arrangements with other countries to share information about people who are on or should be on watchlists. Is that correct?

Mr. LEITER. Absolutely, Senator.

Senator LEVIN. How many people were recommended for the watchlist the way he was by our embassy that were not added to the watchlist in 2009?

Mr. LEITER. Senator, I will have to take that for the record. I will say it is quite routine that the field simply makes a blanket recommendation for an individual's inclusion in all levels of the

watchlist, and it is the headquarters components that then apply those standards to figure out if that individual qualifies.

Senator LEVIN. I understand. I just want to know approximately how many people were recommended to go on the watchlist by our own people in our embassies that were not added to the watchlist.

Mr. LEITER. And, Senator, I will take that for the record. I honestly do not know.

Senator LEVIN. You do not have that approximate number with you?

Mr. LEITER. No, sir.

Senator LEVIN. All right. How many that were on the watchlist last year, approximately, were allowed into the country?

Mr. LEITER. A very significant number was on the watchlist. Just to give you a snapshot, of course, the watchlist is approximately 400,000 names. Out of those, I believe only approximately 14,000 were selectees and only 4,000 no-fly's. So a very significant number, had they traveled to the United States, at most would have been met at the border with some sort of secondary inspection.

Senator LEVIN. It would have been a large number that would not have been allowed in.

Mr. LEITER. It would have been a very large number eligible to come in. Whether or not they were ultimately turned away at the border, I cannot give you that number.

Senator LEVIN. That is sort of instinctively troubling, is it not?

Mr. LEITER. Senator, I think in one way it is, and I think that goes right back to the standards, which are the standards. Have we set the standards so low that we really have too high a bar to get somebody onto the No Fly and Selectee Lists before they get to our shores.

Senator LEVIN. I am talking about the watchlist who were allowed—we do not know exactly how many came into the country who were on the watchlist.

Mr. LEITER. No. I will tell you that when people come to the country if they are on the watchlist, it is because we have generally made the choice that we want them here in the country for some reason or another.

Senator LEVIN. All right. The White House report says that ultimately placement on the No Fly List would have been required to keep Mr. Abdulmutallab off the plane inbound from the U.S. homeland, that he would have had to have been on the No Fly List, according to the White House report. However, in the next section of that report on the visa issue, the report acknowledges that Mr. Abdulmutallab's visa might have been revoked if he had been successfully watchlisted.

Now, if his visa had been revoked, he would have been prevented from boarding the plane. So is there not an inconsistency in those two comments in the White House report?

Mr. LEITER. No, sir, because, in fact, as a general matter, individuals who have had their visas revoked, this may not be known to the people who put them on the aircraft. So not only must the visa be revoked, in many instances they must also be placed on the No Fly List.

Senator LEVIN. And that is not automatic.

Mr. LEITER. I would be happy to talk about it more in closed session, those processes are being modified.

Senator LEVIN. That is a classified question as to whether someone whose visa is revoked is automatically put on the No Fly List.

Mr. LEITER. I can tell you the processes have definitely been changed.

Senator LEVIN. Not the process. I am saying that is the goal.

Mr. LEITER. Yes. The goal is to make sure that anyone who does not have a visa does not get on an airplane.

Senator LEVIN. And the process is intended to achieve that goal.

Mr. LEITER. Correct.

Senator LEVIN. OK. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Levin. Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL

Senator MCCASKILL. Thank you, Mr. Chairman.

To some extent, if any of this has been covered I apologize, but I want to make sure I understand about—and maybe you guys are not the right witnesses for this, and this may not even be the right Committee for this. It may be the Armed Services Committee, but the decision as to where terrorists that try to do our country harm, where they are tried and where they are processed. And I want to make sure I understand what the precedent was before December 25, 2009.

It is my understanding that there is no precedent in this country that anyone has ever been apprehended on our soil for a terrorist act and immediately gone into the military system. Is that correct? Do you all know?

Mr. BLAIR. I think the right witness is from the Department of Justice, Senator McCaskill. I do not know the answer to——

Senator MCCASKILL. It is my understanding that, obviously, a number of terrorists have been prosecuted in civilian courts in this country and that there were a couple under the Bush Administration that ultimately were taken to military court, but after they were initially arrested and arraigned in our civilian criminal courts. And I guess what I am trying to figure out is the process here and if we have a process.

It is my understanding, Mr. Blair, that earlier you testified that you were not consulted about the decision as to whether or not this terrorist was going to go through a civilian court or through a military court.

Mr. BLAIR. That is not quite right, Senator. I was not consulted whether the high-interest interrogation group was deployed so that the questioning of Abdulmutallab would be either admissible in Federal court or was being exploited for intelligence purposes. That is related to where they would be tried, but not exclusively. We would like to be able to do both. We would like to get the information that would help us for intelligence purposes and have evidence that could be used against the person in a Federal court. If we have to make a choice, then that ought to be made at a higher level with all of the considerations that you are talking about.

Senator MCCASKILL. Well, I think my sense is what the American people want is for our military and our intelligence and our

law enforcement community to have all the tools possible to get both good information and justice.

Mr. BLAIR. Exactly. That is the goal.

Senator MCCASKILL. And I think all the tools are very important, but I think we are going to lose the ability to use all those tools if we do not reassure the American people that there is a process in place that these decisions are being made with the right people in the room.

I do not mean to be derogatory to my friends at the Justice Department, but I have had experience in my life where FBI takes over and nobody can talk to them. They just take over. And what I am worried about is can we reassure the American public that at these moments of decision—now, it is my understanding also that this suspect was not Mirandized for a long period of time.

Mr. BLAIR. Not for the initial interrogations, that is right.

Senator MCCASKILL. And the reason he was not Mirandized is, first of all, we did not need his confession or his statements because we had plenty of witnesses in terms of prosecuting him; and, second, we had an opportunity to get more actionable intelligence information by not Mirandizing him.

Mr. BLAIR. I do not know if the decision was made on the scene. The interrogation was done, and then the decision was made on the scene again that evidence ought to be taken for trial after consultation which was not complete. So, yes, that is basically what happened, and it should have been a wider process than was being made on those narrow grounds.

Senator MCCASKILL. I am very proud of our justice system in this country. I am very proud of our military in this country. And I know if the two of them work together, we can punish these people the way the American people expect them to be punished, and we can get good information. These are not mutually exclusive goals. But I do think that what is happening, because we do not have enough information about how these decisions are being made, people are assuming the worst, that we are immediately calling a public defender and saying we want to make sure you do not say anything that could incriminate yourself and how can we coddle this guy who tried to blow up these people in this airplane.

Now, I know that is not happening. I have been around too many interrogations to know that "coddle" is not the word that would come to mind. But I think that we are failing in explaining to the American people how this process is working, and I would certainly ask you, Secretary Napolitano, and all of you in your high-level meetings to discuss this process of the decisionmaking at the point of apprehension. If we are going to go down the path of immediately going into military custody—we have never done that before, I do not believe, in this country—then I think we need to flesh that out. And I think even though there are a lot of things we cannot share with the American public because it will hinder our ability to catch the bad guys, there is a process we can share with the American public that they will understand that all everybody wants is the same thing. We want to catch these guys, and we want to put them away where they can never hurt anyone for as long as we can possibly do it. And in some instances, we want the death penalty.

I think that we need to be very clear that we all have the same goal here. This goal should unite our country, not divide it. But it is being used to divide our country because we do not have enough information.

Mr. Chairman, the remainder of my questions I have for closed session.

Chairman LIEBERMAN. Thanks, Senator McCaskill.

We are going to do a quick second round and see if we still have time within the generous commitment of time you have given us to go into closed session.

Senator Carper, though you are aging, you remain very agile. I heard you were on the way and moments away. Why don't you go ahead and ask your questions?

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you very much.

Let me just start off by saying I know one of you pretty well; the other two I do not know, but I know you by reputation. You have excellent reputations, and nothing you have said or done here today serves to demean those reputations. You have handled yourselves well. I appreciate not just your service but your forthright responses to us.

In my old job, the job that Secretary Napolitano and I once shared, one of my cardinal principles was to focus on excellence in everything we did. I was an old naval flight officer, too, for a number of years. There was focus on excellence in everything we did. I used to say to my cabinet and folks on my staff in the governor's office, "If it is not perfect, make it better."

My family and I traveled outside the country over the holidays, once we left here, and I had a chance to see literally thousands, tens of thousands, maybe hundreds of thousands of people trying to move in and out of this country from all directions, going through security, checking their bags, being ticketed, having their identification checked again and again. And I thought to myself, My God, what a challenge to try to know who all these people are, to make sure they are who they say they are, to make sure they do not have on their bodies or in their luggage stuff that is going to harm somebody else. What a challenge.

It has been over 8 years since September 11, 2001, and we have been facing these challenges literally every day since that time. And we have been lucky, but we have been smart. But we are not perfect, and we need to be as close to perfect as we can be. You know that and I know that.

Our job here is to conduct oversight, to point out and help you point out what you have not done well, and to find out what you need to do differently to reduce the likelihood that we will have another guy with something in his shoes or in his underwear coming at us with the intent to do harm.

What do we need to do differently to enable you to do more? We have spent many a day together here several years ago with the 9/11 Commission sitting right where you are sitting giving us a whole bunch of recommendations and ideas. We acted on almost all of them. And I think we have come along and funded pretty well most of them.

It seems to me—and I will close with this—among the mistakes that occurred, one, when a distraught father, came into our embassy in Nigeria to report that his son was going the wrong way, whoever took that information down, as I understand it, may have passed along the information with the name of the person, the son, misspelled, and I am told that created some problems within the intelligence community and made it more difficult for us to connect the dots.

I understand in a back and forth between one of my colleagues and, I think, Admiral Blair that the idea that somebody was using cash to pay for an airline ticket coming out of Nigeria, frankly they do not all have credit cards, and the idea that they are using cash may not be that much of a strange thing.

The idea that this person had no luggage coming out of Africa with a one-way ticket, or maybe it was a round-trip ticket, I could understand how in Nigeria that might not raise a lot of eyebrows. Maybe it should have in Amsterdam, but if we had the right spelling of this guy's name and if somebody along the line maybe in Amsterdam had picked up that this was a cash purchase and there is no luggage, that maybe should have helped us.

The last thing I want to say is on the full-body scan, the technology side here. We have a pretty good idea how to stop guys like this fellow that tried to blow up the plane over Detroit. The technology is there. I know there are privacy concerns. I think they could be addressed, have been addressed. We need to buy them, we need to fund them, and we need to deploy them. We need to make sure that the folks that need to be trained to use them properly with respect to private sector, that they are in place.

Now, what can we do to help?

Secretary NAPOLITANO. Well, Senator, I will just say thank you for your comments, and I think that there will be budget implications moving forward looking at that.

Second, my view is that—and I want to go back to a point that Senator Akaka asked me, the privacy versus security issue that gets raised in connection with the whole-body scanners. We do, as I said, look at privacy issues from the get-go, but ultimately the question is what do we need to do to protect the security of the flying public, even as we take some measures to deal with privacy. But security is the No. 1 concern.

One thing that this Committee and the Congress can do, however, in addition to that is setting public expectations. We are doing and will continue to do everything we can to prevent this kind of event from ever happening again from whatever source, anywhere around the world, domestically. But there is no one silver bullet.

Yes, we can push some more State Department material out to nine airports around the world, and we have. But even if we had, that is just a tool for additional screening. That does not necessarily prevent someone from getting on a plane.

Yes, we can put more people into secondary screening, but that totally clogs up the travel system unless that is informed by intelligence that has been connected.

So helping the public understand that everyone is working on this, there are multiple layers involved, but no single one will be the sole answer. If there were, it would already be employed.

Senator CARPER. Mr. Leiter.

Mr. LEITER. Senator, I will offer a couple of comments. And as a former naval flight officer myself, I appreciate that if you have a bad day, it might be your last day. And I can tell you that the men and women who are doing this counterterrorism mission feel that way. And, frankly, the hardest thing about this entire experience for our organization has been the people saying, this is not a 9 to 5 job. I have not met somebody who thinks it is a 9 to 5 job yet.

But in terms of specific actions, I think the issue about standards for inclusion in the watchlist and the need to have a good conversation between the Executive and the Congress on determining what that balance should be between security and civil liberties is incredibly important, and this Committee plays a key role in helping us set that spot and that balance.

Second, I think screening, as Secretary Napolitano knows so well, remains critical. It is a critical tool because, frankly, I simply am not going to find all the bad guys. And I do not want us to overlearn the lessons of this case where we did have pieces and we should have connected on Umar Farouk because there will be other instances where with a different name, a different passport, we might not identify them. So we need to have that multi-layered defense.

Finally, in terms of making sure we learn lessons from several incidents and not just one, going back to issues of Fort Hood and domestic radicalization, we have to—and the Congress plays an enormously important role in ensuring that our American Muslim population understands that we need a partnership between the government and these communities to identify individuals like Nidal Hasan or Carlos Bledsoe before they actually pick up a weapon or pick up an explosive and strike. That is not a lesson directly out of December 25, 2009, but I think as we see a morphing threat—and we need the same agility you showed in jumping in your chair—we need to be agile, and that is going to require a partnership with these communities and not an adversarial relationship. And I believe the Congress plays a critical role there.

Senator CARPER. Closing words, Admiral Blair.

Mr. BLAIR. Sir, I would just add the request that you continue to keep the pressure on us.

Senator CARPER. That I promise we will do. That is an easy one.

Mr. BLAIR. Well, frankly, I think the pressure was sort of going the other way in the last couple years: "Things are going pretty well. You have too many people on the No Fly List. Why are you searching grandmothers? These guys are broken up."

I think we are really learning from this incident, in which, thankfully, nobody was killed, and we will make a tremendous leap forward. Of course, the tragedy of September 11, 2001, impelled us to do things that have made a great deal of difference. The trick, as you know from being an executive, is how to keep the pressure on when the crisis does not happen. And I think congressional oversight, I think leadership from our point of view have to be the

keys to doing that so that it does not take a near tragedy or a tragedy to make the improvements, but we make them as we go.

Senator CARPER. Mr. Chairman, I think that is a good note to end on. Thank you very much.

Chairman LIEBERMAN. Thank you. I agree with you, Senator Carper. I appreciate the statement that was made, and I agree that in different ways there may have been not quite a "Mission Accomplished" feeling around Washington, both branches of government, but a feeling that the war had reached a different level of intensity. It has not, and as the records show, we had a greater number of attempts to attack our homeland last year than in any year before. So it was a painful way to be awakened, but here we are.

I appreciate very much the forthrightness of the witnesses today. Like a lot of other people, I was raised with parental wisdom that everybody either falls or slips in life. The question is how you get up, and most important of all, if you slipped and made a mistake, the only way you are going to deal with it effectively is to acknowledge it, acknowledge there is a problem, and then go on. I think that is the spirit of what your testimony has been today.

I have a couple more questions. I know Senator Collins does as well. I want to come back to the watchlist because I appreciated again, I want to say, Admiral Blair, what you had to say. I think this has gone too much in the other direction, and, of course, we do not want Grandma being harassed, but there ought to be a pretty simple way to stop Grandma from being harassed without leaving out of pre-screening people about whom somebody has information that suggests that they may be terrorists. Again, all we are asking—we are not on the basis of their presence on the TIDE list going to arrest them or convict them. We are going to do a secondary screening to make sure they do not blow up the plane or come to the United States with evil intention. And I appreciate the remarks you have made, Director Leiter.

What is the process now by which the Administration is reviewing the watchlist? We are going to perform oversight here continually. We want to have involvement in this with you. Director Leiter.

Mr. LEITER. Senator, to begin, immediately after the event we took some near-term actions which were looking at categories of individuals, rescrubbing their records, and, frankly, elevating large numbers of people, based on certain characteristics, that I can talk about more in closed session, to at least the selectee level, further scrubs of that involving people with visas and the like, so there were some immediate steps taken.

In the slightly longer term—and I really should not say "long term"—this week—I expect that we will obtain interagency guidance out of this process, so within the next 30 days to more formally revise those standards so we can have routine inclusion of people at higher levels of that watchlisting. And certainly as we develop those standards, which I hope are simple for everyone to understand, we have to engage in real consultation with this Committee and other Members of Congress to make sure that, again, we are hitting the right balance.

Chairman LIEBERMAN. OK. We want to be involved in that. If I may, since you are here, just suggest that it seems to me that the

watchlist system is too complicated, that having four levels—TIDE, watchlist, Selectee, No Fly—may be complicated—is more complicated, in my opinion, than we need. There ought to be a category where there is some basis for concern about contact with terrorism and then some higher category where there is some greater evidence where you really want to stop somebody from getting on the plane.

Mr. LEITER. And, Senator, I have heard that a lot. I can tell you that we have, to a vast degree, eliminated one of those levels, which are those who are on TIDE that are not in the watchlist at the Terrorist Screening Center. Not completely, and I can explain that more fully in closed session, but fundamentally that step does not exist.

I will say that one of the good things about the watchlist is this ability—and this did work in this case. We simply had not watchlisted someone at the right level. But what we do have is something that did not occur before September 11, 2001, which was a seamless connection of information flow from that top secret level at the National Counterterrorism Center down to the screeners.

Now, again, we had a different problem here, which was someone was at the wrong level of the watchlist. But the information did flow so that basic structure was not, in this case, one of the flaws.

Chairman LIEBERMAN. OK. And, Secretary Napolitano, perhaps I should ask you this question because it goes to TSA and maybe CBP. These questions of Grandma getting screened or this young boy, Michael Hicks—the name sticks in my mind. Apparently there is somebody on one of the lists with a similar name getting screened all the time. There has just got to be a common-sense way when there is a little boy coming through to not subject him to this. It is not a terrible price to pay, frankly, to protect the country, but we ought to try to avoid it if we can.

Secretary NAPOLITANO. Indeed, Mr. Chairman, but I can talk about that particular case in a classified setting.

Chairman LIEBERMAN. OK.

Secretary NAPOLITANO. What we are going to have to build or have as we make the actual watchlist and No Fly List more robust is a greater ability to have redress and remove people who are improperly on the list from the list and a clearly understood non-bureaucratic process by which to do that. That is something we are looking at.

Chairman LIEBERMAN. OK. Let me ask you a question about how the lists are used, and Senator Levin touched on this, and you have described it. This is a question of pre-screening of international air travel passengers to the United States. In the current system, Customs and Border Protection accesses the airline's passenger name record 72 hours before a flight is set to depart. But those records do not typically include important identifying information like passport or visa numbers, which obviously makes it harder to match the passenger manifests with the government databases, the terrorism watchlists.

Customs and Border Protection currently does not receive that important identifying information about passengers on a U.S.-bound flight until they begin the check-in process and in some cases not until 30 minutes before the airplane's door closes.

Also, although we are checking the No Fly and Selectee Lists in real time as passengers check into a flight, we are not running, as we described earlier, visa revocations in real time.

Now, once the airplane's door closes and CBP receives that batch of passenger information, officials at what we call the National Targeting Center begin a more in-depth analysis of the people on the flight to determine who will require additional attention once the flight lands.

On Christmas Day, as you know, it was that in-depth analysis that led CBP to uncover Abdulmutallab's father's concern about him and to determine that he would require a secondary inspection once he landed in Detroit, but, of course, that was far too late to stop what he intended to do.

So I wanted to ask you whether waiting until the airplane's doors are closed to begin an in-depth check of our databases is too late and whether we need to thoroughly screen each flight's passenger manifest list against all of our databases, such as we have described, at least 24 hours, if not longer, before the airplane is set to depart a foreign country to the United States.

Secretary NAPOLITANO. Mr. Chairman, I think some of that should be held for our classified briefing in terms of how that flow of information works. Obviously, where we want to get to is if we have derogatory information that someone is a threat to aviation, they never get on a plane.

Chairman LIEBERMAN. Right.

Secretary NAPOLITANO. The problem here is when they put all the dots together, that derogatory information was enough to advise the carrier not to put him on a plane. That was the problem here.

In terms of the entire movement of information across the system with the millions of passengers that move every day, I would like to be able to talk with you about that a little more in-depth in the classified setting.

Chairman LIEBERMAN. You understand my point.

Secretary NAPOLITANO. I do.

Chairman LIEBERMAN. That if prior to boarding the plane what we have is basically the passenger identifying information—that is, his name, or her name—but not other information like passport or visa numbers, it may be that we are not going to be able to effectively match them on that basis against the watchlist, and, therefore, they will get on the plane. But we will continue this conversation. Thank you.

Secretary NAPOLITANO. Indeed.

Chairman LIEBERMAN. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, before I ask a couple of final questions, I want to clarify an issue raised by the Senator from Missouri, and I told her as she was leaving I was going to do this. There is, in fact, precedent for detaining someone on American soil as an enemy combatant in the military system, and that is Jose Padilla. Jose Padilla was first arrested in 2002, and he was subsequently detained by the military for 3½ years before being charged in civilian court. Whether that was the right way to handle the case or not, it is indeed a precedent. So it would not have been unprecedented

to detain Abdulmutallab, who, unlike Jose Padilla, was not an American citizen. So that could, in fact, have been done and would not have been unprecedented.

The second point my friend from Missouri raised had to do with the amount of information that was given by Abdulmutallab. That is obviously classified and not for discussion here. But it is evident to me that you are going to get more information over a lengthier period of time than you are over just a few days, and it is clearly not a coincidence that Abdulmutallab stopped cooperating once he had his Miranda rights read to him and once he had lawyers who advised him to cease answering questions. So I have a very different view from my friend from Missouri on this issue, but I did want to establish some facts on Jose Padilla as being a precedent.

I want to follow up with another issue with Mr. Leiter that Senator Levin raised, and this is just to clarify the record. On the terrorist watchlist that contains 400,000 names, you had an exchange, Mr. Leiter, with Senator Levin in which you and he talked about potentially significant number of those individuals would be able to travel to our country because they are not on the No Fly List or even the Selectee List. But, in fact, as I understand it—and, again, I realize the actual number is classified, but very few of those 400,000 would have valid current visas. Isn't that correct?

Mr. LEITER. That is correct, Senator, but approximately 2 percent of the people who are in the Terrorist Identities Datamart Environment (TIDE) are U.S. persons, so clearly that is an issue. Also, there are a significant number that are from visa waiver countries and could enter the United States without a visa.

Senator COLLINS. That is an excellent point, and it is a point that has been of great concern to the Chairman and me for some time, particularly when we are looking at individuals in Great Britain who may have dual citizenship with Pakistan and England and may be using one passport to travel to Pakistan and then the British passport to travel to our country. I realize that is an issue for another day, but it is of great concern.

Mr. LEITER. Well, I actually do not consider it an issue for another day because, as I said, we have to learn the lessons of this case, but we cannot overlearn the lessons. And I think Secretary Napolitano and I have spoken previously and view the issue of visa waiver and using Electronic System for Travel Authorization (ESTA) data appropriately to detect individuals who might want to do harm to the United States is very much integrated in this equation.

Senator COLLINS. Secretary Napolitano, in my remaining time let me ask you about a question that concerns me. When DHS was established in 2002, Congress authorized the Secretary of Homeland Security to assign DHS personnel to visa-issuing diplomatic posts overseas to review individual visa applications and to initiate investigations of visa security-related matters. Well, fast forward 8 years. It is 8 years later, and as I understand it, DHS personnel are only in about 15 out of the 220 State Department posts around the world. And that small number is even more disturbing when you consider that DHS and the State Department have identified 57 posts as being high risk.

I also understand that requests to expand to three more of these high-risk posts were waiting in your office for more than a year, waiting for approval by the Secretary—I realize part of that preceded you, but you have been in that office for about a year—and that you signed them just recently.

Why the delay? Here you have a need in a high-risk area for DHS personnel. Why let it languish for a year?

Secretary NAPOLITANO. It was not languishing, Senator, and let me talk about this in several ways. It was being evaluated in light of all the work being done at the Department about where our people need to be to have their highest, most effective use around the world, and in conjunction with the work we were doing on the Quadrennial Homeland Security Review (QHSR), which is due to the Congress this month.

Let me, if I might, though, talk about the Visa Security Program. Senator Carper asked, what we could do. Well, both at the IAP level and at the Visa Security Program level, there is a difficulty, and the difficulty is that they make the Department a little bit pregnant. Either we run visas or we do not. Either we do the revocations or we do not. But we live in kind of a half-caste world right now, and I think it is important—and that is something that we ought to be—that is part of our review, but it also should be part of our ongoing dialogue with this Committee.

Last, the Visa Security Program is a screening/investigative program where, in the embassies where we have it, with the agreement of the Department of State, they go out and do further research. But as you have mentioned, it is limited. It does not cover all of the embassies, nor can it by itself be more than and should be more than one of the many layers to be constructed here.

So I would simply suggest to the Committee that this is one of the things we really need to look at, and areas of the Department where we kind of have authority but we kind of do not, we kind of have personnel, but we kind of do not.

Senator COLLINS. But you did have the authority to deploy people to these high-risk posts. You had a request for these three, and I cannot publicly say what the three are, but they do not seem like hard calls from my perspective.

If they did not languish for a year, are you saying that it took a year to evaluate the request? I mean, why the delay?

Secretary NAPOLITANO. No. What I am saying, it was not a delay. It was an ongoing process within the Department, led by leadership in the Department to look at this in conjunction with everything else we were doing internationally.

Senator COLLINS. Was the request made a year ago?

Secretary NAPOLITANO. I do not know when the actual date of the request was.

Senator COLLINS. It is my understanding that the request has been in your office for a year, and I will follow up with some additional questions.

Secretary NAPOLITANO. I do not think that is accurate. We will be happy to have some correspondence with you and to get you the information.

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

Chairman LIEBERMAN. Thanks, Senator Collins.

Senator Akaka, do you have any further questions?

Senator AKAKA. Mr. Chairman, I do have further questions, but I know there is a vote.

Chairman LIEBERMAN. There is a vote, but if you would like to start, go right ahead. I think there are about 13 minutes left on the vote.

Senator AKAKA. Well, thank you, Mr. Chairman. This is becoming so obvious now, what has been going on with this Administration and with different agencies and departments working together.

Director Leiter, NCTC has a Directorate of Strategic Operational Planning to support effective governmentwide counterterrorism planning, which is essential to preventing attacks. Yet Congress also directed the State Department's Coordinator for Counterterrorism to conduct overall supervision and oversight of resources for international counterterrorism activities. NCTC's and State's authorities appear from our perspective to overlap.

Are the State Department and NCTC cooperating in counterterrorism planning? And, how are you doing this?

Mr. LEITER. Senator, I think we are cooperating well, but I would go back to something Director Blair said earlier. There are so many people involved here, and I do not think the legislation that created NCTC's Strategic Operational Planning, as I have discussed with this Committee before, I do not think the legislation gave clear authority—in fact, it did not give us clear authority to direct action, so we have become a negotiator and mediator of sorts rather than director of action.

I think the President's Directive of January 7, 2010, which asked or directed NCTC to design a process whereby there would be follow-up of priority threat streams, will be empowering of strategic operational planning, not to direct operations, contrary to the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), but at least to empower us to demand accountability at a more tactical level for more, and a broader range of threats than we see. I think that will require a new level of cooperation from the State Department, also not just the State Department, but Homeland Security, FBI, Justice, and the military. I believe the events of December 25, 2009, at least give us the impetus to do that.

Senator AKAKA. Thank you for that.

Secretary Napolitano, the public, of course, has been very concerned about what has been happening, and we are trying to put different measures in place. In your testimony, you state that, as an interim measure, you will deploy law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard some international flights.

When will these officers be deployed? And, what training do they receive to ensure that they are fully prepared to provide security inside an aircraft?

Secretary NAPOLITANO. Senator Akaka, if I might reserve the details of the deployment for the classified briefing.

With respect to training, there is specialized training. Indeed, we have a new, enlarged group that started training this week that will begin deployment on February 1. But it includes things, for example, about how to take down a passenger in a plane and keeping the other passengers safe while you are doing it, because you are

in a closed environment; how to take down a passenger in a plane without yourself causing damage to the structure of the plane. There are other things, but that gives you a flavor. There are some different things from a law enforcement perspective that happen in that airplane setting that are different than a normal setting.

Senator AKAKA. Finally, this came to me while you were talking about working with other countries. You testified that TSA's security directive requires passengers who are from or who pass through 14 countries to undergo additional screening at international airports prior to being allowed on flights to the United States. I am concerned that requiring additional screening of all passengers from certain countries may impact our relationships with those countries as well as the countries charged with providing the additional security and could divert attention from other possible threats.

Have you heard concerns about this directive from other nations? And what is being done to address those concerns?

Secretary NAPOLITANO. Senator, that list was developed from the State Department's state sponsors of terrorists list plus add-ons to it in conjunction with the State Department. It is of concern to several of the countries that have been put on the list, recognizing that the enhanced screening is happening for over half of the passengers from all other countries who are embarking for the United States.

So this is a very aggressive, very all-inclusive method. Nonetheless, we are talking with members of some of those countries and talking about ways or things that they could do that would alleviate concerns and allow them to be removed from the 100 percent list and go onto the list where we still do over half of the passengers.

Senator AKAKA. Thank you very much for your responses. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka.

I would say to the witnesses that there is a vote on the floor now, and you have been really generous with your time. So I think it would be a mistake to go into the classified session now. It would take more of your time. We will try to reschedule it. It is even possible, in the spirit of cooperation and one of the unadopted recommendations of the 9/11 Commission Report, that we might sit in with another committee in a closed session with the three of you.

I want to thank you—incidentally, just to say in public session, I know it is controversial. I have heard pushback from some of the 14 countries, but stay tough on this. I am just saying that what is on the line here is so critical, which is the life and death of Americans, that, yes, it is inconvenient but, again, basically you are talking about just some more screening before you get onto a plane. It is done to achieve a public good. So I think you started out with the right position. I have already had people, friends of mine in other countries, complaining about it. But that is the world we live in.

Secretary NAPOLITANO. Indeed, Mr. Chairman. And as I responded to Senator Akaka, our job is to make sure that the air environment is as safe as it can be.

Chairman LIEBERMAN. Good. I appreciate it.

Again, I thank you. You have been forthright. We are in a world war with the Islamist extremist terrorists who attacked us on September 11, 2001, and have been coming at us in various ways from a diversity of places ever since. You had a little exchange with Senator McCain before. I think one thing we all agree about war is that mistakes are constantly made, and when they are made and when the enemy breaks through your defenses, immediately you are tough about it, as you said; you close the gaps. You do hold people accountable, as is appropriate, and you go on with the aim of securing the country that we are all here to defend and the freedom that we are all here to defend.

So it is in that spirit that I appreciated very much your testimony. We have covered a lot of ground. We have learned a lot. I appreciate what you are involved in now to fix what did not work in these cases. And we are going to keep going with these oversight hearings. Next Tuesday we will have Tom Kean and Lee Hamilton and some other witnesses, and we are going to then go on to separate subject matter hearings in this oversight. We will issue some recommendations. But we want to work with you every step of the way. We obviously have a common goal, which is the greatest possible homeland security for the American people.

I thank you very much. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. We are going to keep the record of the hearing open for 15 days for additional questions and statements from the Members. With that, I thank you again. The hearing is adjourned.

[Whereupon, at 12:13 p.m., the Committee was adjourned.]

INTELLIGENCE REFORM: THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK—PART II

TUESDAY, JANUARY 26, 2010

U.S. 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, Carper, Burris, Kirk, Collins, McCain, and Bennett.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order.

Good morning and welcome to this second in a series of hearings during which our Committee will examine how the intelligence reforms passed by Congress in the wake of the attack of September 11, 2001, are working, and examine the reforms in the light of recent terrorist attacks and the ongoing threat, and what parts of what we have done earlier may perhaps need further reform so that we can fulfill our responsibility to protect the homeland security of the American people.

I want to just go back to last week's first hearing in this series of hearings before I focus on this one and say that I very much appreciated the fact that all of our witnesses in last week's hearing—Director of National Intelligence Dennis Blair, Director of the National Counterterrorism Center Michael Leiter, and Department of Homeland Security Secretary Janet Napolitano—acknowledged that mistakes were made with regard to the Christmas Day attack on the plane over Detroit, and all three of them offered to work with each other and with this Committee to make our existing multi-layered counterterrorist defenses quicker to react and harder to penetrate.

I thought Admiral Blair was especially forthright, and I thank him for that. My guess is his forthrightness has probably brought him some criticism and made him the target of some displeasure, but it was definitely the right thing to do because it was the way he felt and he spoke in what he believed to be the national interest. It is self-evident that our homeland security intelligence and law enforcement agencies did not work as we on this Committee—and as Governor Kean and Congressman Hamilton in their work post-

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00057 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

September 11, 2001—would have wanted those agencies to work. The point is that unless the people in charge admit that, as our three witnesses did last week, the problems will never be fixed. And when they do deal with their shortcomings forthrightly, then we have some hope that the problems will be fixed, and obviously whatever mistakes were made will not recur again.

I do want to say that one of the most troubling revelations at our hearing last week was that none of the three witnesses was consulted before the Christmas Day bomber was turned over to our criminal courts rather than to the military where I believe he should have been held, since he was trained, equipped, and directed to attack America by al-Qaeda.

Now, the fact is that since our hearing last week, Osama bin Laden himself has boasted of al-Qaeda's sponsorship of the Christmas Day attack on America. And so while al-Qaeda claims credit for this attack, Umar Farouk Abdulmutallab, whom I think we can fairly describe as a soldier in al-Qaeda, and obviously not an American citizen, now enjoys the constitutional protections of an American citizen, including a lawyer who immediately counseled him to remain silent, even though he may have information that could protect the American people from another terrorist attack. To me this is outrageous—a kind of "Alice in Wonderland" situation turning the world of common sense on its head.

And that is why yesterday Senator Collins and I wrote to Attorney General Holder and Deputy National Security Adviser Brennan, urging them to immediately turn Abdulmutallab over to the Department of Defense, where he can be held as an enemy combatant, as a prisoner of war, which he is, acknowledging with some certainty and gratitude that this also means that he will be held and given rights far in excess of what the Geneva Convention requires enemy combatants or prisoners of war be given. Senator Collins and I, and our Committee, are going to stay on top of this and other aspects of it to make sure that this mistake, the failure to consult with intelligence and homeland security officials before deciding how to handle Abdulmutallab and then the decision to turn him over to the civilian courts, is never made again.

I do believe our homeland security intelligence gathering and analysis have remarkably improved since the attacks of September 11, 2001, and that the sharing of intelligence, as we said last week, at all levels of government is vastly improved. This is due in no small measure to the work of two gentlemen who we are proud to have as our witnesses today: Chairs of the 9/11 Commission Governor Tom Kean and Congressman Lee Hamilton. The passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) has played a critical and extremely positive role in driving the changes that make the American people more secure today than they were on September 11, 2001.

It is the work of these two gentlemen that leads us in part to refer to the Act I have just referred to as the 9/11 Commission Act—in part that is the reason. The other part is that it sounds a lot better than saying IRTPA, which is the acronym. The fact is that Act implemented most of the bipartisan recommendations of the Commission, and Governor Kean and Congressman Hamilton have been unique, not only in their bipartisan service in this re-

gard on the Commission, but in continuing to track the implementation of their recommendations persistently over the last 5 years.

They are testifying before us today in their current capacity as co-chairs of the National Security Preparedness Group. I welcome both of you, and I thank you very much for your service.

Your 9/11 Commission's recommendations were comprehensive, both in terms of long-term actions we can and should take to blunt the terrorists' appeal and to stop their ability to recruit, and also more short-term actions that we need to take to defend our Nation against further attacks.

One of the challenges revealed in our hearing last week was the overwhelming amount of information that is collected by our intelligence and law enforcement agencies for analysis. It has been estimated, as you gentlemen know, that the National Security Agency alone collects on a daily basis four times more information than is stored in the Library of Congress. Hard to imagine, but that is how much is being collected.

I know that Governor Kean and Congressman Hamilton have been considering this challenge, and I will be interested to hear their thoughts on how we can better organize our intelligence-gathering and analysis efforts so that crucial information can be mined more quickly from the vast mountain of data we build. I mean, after September 11, 2001, we were saying, correctly I believe, that the dots that we were collecting did not come together on the same board, as it were. I think now, thanks to your recommendations and the legislation that followed, the dots are coming together on the same board. But there are so many millions, billions of dots, the question is how do we see the patterns to help us act preemptively to stop attacks against our country.

Another question I would like to explore in more detail with our witnesses relates to the authorities that we provided to the Director of National Intelligence and the National Counterterrorism Center in the 9/11 Commission Act. Bottom line question: Do we need to give the Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC) additional authorities, or do we need to push them harder to use the authorities they already have?

And, again, I know that the two of you have done some preliminary work on this, and I look forward to the guidance that you can offer our Committee as we go forward with this series of hearings which is aimed at coming up with a status report and perhaps recommendations for legislation or further executive action.

I cannot thank you enough for your unflagging efforts to secure our Nation against terrorism, particularly Islamist terrorism—a rootless and shadowy enemy, driven by theological extremism and unbound by any sense of morality or respect for life. That is the challenge of our time, and because of your extraordinary service, we are doing a lot better than we otherwise would have done in meeting that challenge.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. I, too, join in welcoming our two distinguished witnesses back to our Committee.

But for their efforts and the efforts of the families of the victims of September 11, 2001, many of whom are also here today, we would not have accomplished as much as we were able to.

Nevertheless, we are hearing these words today: "Intelligence failures," "calls for reform," "lack of accountability," "failure to connect the dots"—testimony by Governor Kean and Congressman Hamilton. As Yogi Berra once said, "It sounds deja-vu all over again." But, in fact, there are significant differences between now and then.

When our Nation was attacked on the morning of September 11, 2001, our intelligence community was hampered by an organizational structure that undermined unity of effort. It was led by a Director that had little authority over its various elements and little incentive to focus beyond the mission of the Central Intelligence Agency (CIA). It was burdened with a culture that promoted parochial agency interests over the intelligence needs of a Nation.

The Intelligence Reform and Terrorism Prevention Act of 2004 fundamentally changed our intelligence community. Working with the families of the victims and with our two distinguished witnesses as well as the rest of the members of the 9/11 Commission, this Committee was able to pass the most substantial reforms of our intelligence agencies in more than 50 years. In fact, my favorite name for the bill is the Collins-Lieberman Intelligence Reform Act. [Laughter.]

In the 5 years since this Act became law, information sharing and collaboration among the 18 elements of the intelligence community have improved dramatically. And in 2009 alone, the intelligence community, working with Federal, State, and local law enforcement and homeland security agencies, has helped to detect and disrupt numerous terrorist attacks targeting our Nation. Two of these successes were the arrests of David Headley and Najibullah Zazi in two separate terrorist conspiracies. Other successes also were made possible in part by the reforms that this Committee spearheaded in 2004.

But, standing alone, a law cannot accomplish transformation. At the end of the day, even the most powerful laws are just words on paper. They rely on the President and leaders within the Executive Branch to produce reform, to aggressively carry out the authority that they have been given. And to fight the war on terrorism, the President, the Director of National Intelligence, the Secretary of State, and other leaders must use the laws we pass to their fullest extent.

Unfortunately, the terrorist attack at Fort Hood and the failed Christmas Day plot are stark reminders of what can happen when those authorities are not used effectively.

Let us just look at some of the authorities given under the 2004 law. The DNI has the clear authority to determine requirements and priorities for the management and tasking collection analysis and dissemination of national intelligence. Yet the initial analysis shows that the DNI failed to respond to the growing threat that al-Qaeda in the Arabian Peninsula posed to the United States and apparently failed to target sufficient resources at this threat.

The Intelligence Reform Act also provides ample authority to "ensure maximum availability of and access to intelligence information

within the intelligence community." Yet intelligence regarding the threat posed by Major Hasan apparently remained stovepiped at a Federal Bureau of Investigation (FBI) Joint Terrorism Task Force instead of being provided to officials within the Department of Defense who might have been able to act to prevent that attack.

Similarly, we saw failure to connect the dots, the streams of intelligence reporting with regard to the Christmas Day attempted attack.

The law directs the DNI to "ensure the development of information technology systems that include . . . intelligence integration capabilities," yet here again the intelligence that may have allowed us to identify Abdulmutallab as a terrorist remained undiscovered in multiple intelligence community databases—disseminated, as the Chairman pointed out, those dots were out there. They were disseminated, but they were not connected.

The law provides the Secretary of State with clear authority to revoke a visa "at any time, in [her] discretion," yet Abdulmutallab's visa remained valid when he boarded Flight 253. It remained valid despite the fact that the State Department had already decided to question him about his ties to extremists if he chose to renew his visa. I would ask: How could he have been a threat to the United States in the future based on these extremist ties, but not a sufficient current threat to cause his visa to be revoked? That defies logic and common sense.

And, finally, despite the President's authority to hold Abdulmutallab as an enemy belligerent and subject him to a thorough interrogation for intelligence purposes, the Department of Justice, as we learned at our last hearing, unilaterally decided to treat him as a common criminal, as an American citizen, advise him of his right to remain silent, and grant him a lawyer at the taxpayer's expense. It is outrageous that our Nation's top intelligence officials were never even consulted on this vital decision. And Senator Lieberman and I introduced a bill last week to try to prevent that from ever happening again.

My point is that the President must empower his senior officials to use every authority available to them to defeat the terrorist threat. Doing so does not require action by Congress. That is not to say that further reforms are not needed, but correcting those problems is possible under the current law. It is just a matter of using the authority. They do not require a 60-day review or more studies. They should be implemented now. Nothing less than the security of our Nation hangs in the balance.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

I also want to note with gratitude the presence of members of the families of some of those we lost on September 11, 2001, whose persistence has not just matched those of Governor Kean, Congressman Hamilton, and Members of Congress, but really surpassed it. And it is just great that you are here. They are in the front row, various organizations, particularly Voices of September 11th. We thank you, and we are going to stick with it. I have often said it but it is true. If it was not for these folks, we never would have had the Commission. If it was not for the Commission, we never would have had the legislation. So thank you.

Do you two toss a coin as to who goes first in the spirit of bipartisanship?

Mr. HAMILTON. I will go first.

Chairman LIEBERMAN. Congressman Hamilton, it is great to see you and welcome.

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

Mr. HAMILTON. Well, good morning to the Committee, and thank you very much for inviting Governor Kean and myself to be with you again. We are very cognizant, of course, of the fact that were it not for this Committee, many of the recommendations of the 9/11 Commission would never have been enacted. Really, the Committee has shown extraordinary leadership on these questions over a period of years, and I know that the country is safer, and the country should be very grateful because of the work of this Committee. We thank you for it.

Senator Lieberman, I want to say that you are exactly right about the families. This law would never have come into effect had it not been for them, and Governor Kean and I have had a marvelous relationship and support from them over a period of years.

As you suggested, we are appearing today because of the Bipartisan Center's National Security Preparedness Group. Our written testimony gives the membership of that group. I will not go over them. I know their names are familiar to you. But it is an extraordinary group of national security professionals that joined Governor Kean and me in this review of the 9/11 Commission recommendations.

At the National Security Preparedness Group, we have been studying the implementation of the 9/11 Commission recommendations. We are still pretty early on in that review. But we do have at least some tentative conclusions to present to you today.

The Christmas Day event and Fort Hood, as well, give us the opportunity to make two important points. One is an obvious one, but still very important, and that is that the threat from al-Qaeda and radical Islam remains very strong.

One of the members of our group—you know him by name if not personally—Bruce Hoffman has observed that "al-Qaeda is on the march, not on the run." And all of us agree with that. We have expressed, Governor Kean and I, over and over again our sense that the urgency on terrorism has been too low, and we have to reject complacency and recognize that we still confront a very serious threat. That is not a reason for panic, but it certainly is a reason for a comprehensive, concerted effort.

The second observation we would make is that we see that the determination of the terrorist to attack the homeland remains unabated, but it reminds us of the need for establishing the Director of National Intelligence and the National Counterterrorism Center in the first place. We need to support these entities and

[1] The joint prepared statement of Mr. Kean and Mr. Hamilton appears in the Appendix on page 290.

build them into strong and enduring institutions. It is imperative, in our view, that the DNI and the NCTC be successful in their vital missions that they have been asked to undertake for the country.

We have been pleased that your Committee has initiated this series of hearings on how well intelligence reform has been implemented, and that is exactly the kind of congressional oversight that we called for in the report.

There has been a debate within the intelligence community on the state of intelligence reform and the effectiveness of the DNI. The DNI has been hobbled by endless disputes over its size, mission, and authority. We are concerned about the criticism that is sometimes made about the growth and bureaucracy of the DNI, and we support, as I am sure this Committee does, an ongoing vigorous reevaluation of its functions to assure its leanness. But such a review must occur with the recognition that the Congress and the President gave the DNI a massive to-do list, a great deal of authority, as Senator Collins has pointed out, in the wake of the intelligence failures of September 11, 2001, and the weapons of mass destruction.

It is not enough to say simply that the DNI bureaucracy should be reduced. We need to take a fresh look at how the DNI has performed on the essential tasks, clarify the mission, and then seek to adjust accordingly.

In recent months as we have studied the effectiveness of the DNI, we have come to some preliminary conclusions. We have a lot more work to do, but we believe that the DNI has achieved a meaningful measure of success in its first years. It has been worth the inevitable turmoil. But it is a work in progress, closer, I think, to the beginning than the end of reform.

Since September 11, 2001, the NCTC and other government agencies have repeatedly connected the dots and shared the information necessary to defeat terrorist attacks. Improvements have clearly been made on this point of sharing the information, although we continue to believe that sharing is not as prompt and as seamless as it should be.

But many of the successes of the DNI have been heavily dependent on key personalities within the Executive Branch, both under the Bush Administration and the Obama Administration. We want to continue to look closely at the authorities of the DNI to make sure he has the authority to do his work, but it is our sense that the success of the DNI in the short term will not rise or fall on whether we make additional statutory adjustments to the Intelligence Reform and Terrorism Prevention Act. In other words, that was a difficult piece of legislation to get enacted. It is on the books now. It is going to be the governing statute for a period of time, probably a long period of time, and so you have to work with it.

I think there probably are some ambiguities in the law, although you can argue, as I think Senator Collins was doing in her opening statement, that it is more a failure of exercising authority than ambiguity. But certainly, for example, Section 1018, the passage designed to ensure the chain of command in departments and agencies will not be abrogated—that is a provision in the law—raises some question of authority. And certainly there have been some problems resulting from that section. We hope those have been

cleared or at least improved by Executive Order 12333 put into effect in the final weeks of the Bush Administration.

Now, the greatest challenge facing the DNI then relates to his authorities and his role. From my point of view—and I think from Governor Kean's as well—the burden is clearly on the President to be very specific as to who is in charge of the intelligence community and where final authority lies on budget, personnel, and other matters. Now, obviously you need a strong DNI as a leader of the intelligence community. That person has to drive interagency coordination and integration, which we all know in this intelligence community is a massive task.

At the same time, the DNI's authorities must be exercised with discretion and consideration of the priorities and sensitivities of the other intelligence agencies. You really do need a diplomat in this job because you have 16 strong-willed agencies that are involved. But the President's leadership is the key. It is crucial and must be continuing, or we run the risk of mission confusion and decrease the prospect of the long and lasting reform that was recommended after September 11, 2001. The DNI's ability to lead the intelligence community depends on the President defining his role or her role and giving them the power and the authority to act.

Chairman LIEBERMAN. Thank you very much for a very strong and thoughtful statement. Very helpful to the Committee.

Governor Kean, thank you. Welcome back.

Mr. KEAN. Thank you, Mr. Chairman, and I will just echo something Mr. Hamilton said. I remember when we were all lobbying to our best to get this massive bill passed, and I talked to one of your colleagues, and they said, "This bill is going to pass. You know why?" And I said, "Why?" And he said, "Because of the leadership that has taken control of this bill in the Senate. Because of the respect for them, this bill is going to pass." And so thank you. Thank you very much for your leadership in that area and, of course, again the incredible families of September 11, 2001. They were the wind in our sails on the Commission. They are still with us every day. They are still supporting the other families. They are still here lobbying to make this country safer. And every time I come here and see them—they are here more than I am, and I just echo Mr. Hamilton—and the Committee in saying thank you so very much to Mary Fetchet and to all of you.

Much has been said about the lessons from the Christmas Day attack. I would like to highlight just a couple of issues.

First, the greatest single challenge that arises from this incident, in our view, is the urgent need to strengthen the analytic process. The President himself said there was a failure to connect the dots. With more rigorous analysis, we might have been able to connect disparate pieces of information, and that, of course, might have foretold that Christmas Day plot.

We are pleased the President asked the DNI to look at this issue. The DNI was charged by you to ensure the highest analytical standards within the intelligence community. The DNI is properly situated within that community to assume a leadership role in applying the most rigorous standards to their analytical tradecraft.

Congress should also support these entities by giving the DNI and the NCTC the resources they need and, above all, the ability to recruit and to keep the very best people available.

Another part of improving analysis is judging sources of potential attacks properly. As the President's review has shown, we had what he described as "a strategic sense" that al-Qaeda in the Arabian Peninsula (AQAP) was becoming a threat, but, again, "we didn't know they had progressed to the point of actually launching individuals here."

Now, we collect an enormous amount of intelligence, and we need the very best people not only sorting through it for tactical details, but in a strategic sense taking that and sort of making a decision as to where is the next attack liable to come from and what is happening out there.

You talked about more information coming in, Senator, than in the Library of Congress. It is absolutely incredible what comes in every day, and the intelligence community is awash with data. So in this age when we are collecting more information than ever before, the real challenge is how do we understand it, how do we manage it, how do we integrate it. The DNI needs to develop ways of dealing with intelligence information overload. At the same time, we need to do a better job of pushing information to the right people within the intelligence community. We welcome President Obama's order to distribute intelligence reports more quickly and more widely. We need better management of the data and to look to technology to help us better sort through massive amounts of information to ensure that the right people are seeing it, and seeing it in time to make a difference. The technology we use must be state of the art, must be constantly upgraded to quickly put information together, and it must be properly placed instantaneously so better analysis can occur.

We heard a number of times during testimony back 5 years ago before the 9/11 Commission that the analysts were sometimes treated as second-class citizens in the intelligence community. Hopefully that is not happening today. But these people are probably if not the most important, among the very most important people in the whole community, and we should do everything we can to support them, to value their professionalism, and to get the best of them to stay in government and to attract others like them to the same job.

A second lesson from the Christmas Day attacks is that it reminds of the importance of eliminating terrorist sanctuaries. When we found out that the attackers from September 11, 2001, benefited so much from the time, space, and command structure that existed at that point in Afghanistan, the 9/11 Commission placed great emphasis on identifying and prioritizing actual and potential terrorist sanctuaries. We recommended strategies employing all elements of national power because the more we can keep terrorists insecure and the more we can keep them on the run, the better off we are, the less able they are to attack us. We are very fortunate that the attack on Christmas Day emanating from Yemen did not succeed, but this episode reminds us again, let us look where are these people developing sanctuaries.

Again, Bruce Hoffman, our colleague, observed, al-Qaeda is aggressively seeking out, destabilizing, and exploiting failed states and any other area they can find of lawlessness, and over the past year has increased its activities in places such as Pakistan, Algeria, the Sahel, Somalia, and, of course, Yemen. The United States should take a fresh look at these areas and deepen our commitment to ensuring al-Qaeda cannot exploit those territories to launch attacks on our homeland.

Then just a couple of matters that are left over in a sense from our report. We have talked a number of times, all of us, about balancing the need between civil liberties and national security, and we have to get that balance right. It is absolutely important. To do that, we recommended and you enacted a Civil Liberties Board located in the White House which would look at the implications of whatever laws were passed from a civil liberties point of view. That board was staffed and became operational in 2006. Congress further strengthened it in 2007, made it an independent agency outside the White House.

Now, the board held at that point numerous sessions with national security and homeland security advisers, the Attorney General, and the FBI Director, among others, on terrorist surveillance and other issues that might arise from the collection of information.

But that board has disappeared. It has been dormant since that time. We have now a massive capacity in this country to develop data on individuals, and the board should be the champion of seeing that collection capabilities do not intrude into privacy and civil liberties. We continue to believe, Mr. Hamilton and I, that the board is critical in the overall functioning, and we urge President Obama to reconstitute it, to appoint its members, and to allow them once they are appointed full access to the information and the authority to perform what we consider an essential function.

Let me give you one more leftover recommendation from the 9/11 Commission Report. When those of us who are citizens come down to Washington and we want to find out about transportation, environmental protection, or education, we can go and we can hear from the various committees, and we listen and we can participate as much as we can as citizens as part of our democracy. For a lot of the information on intelligence we cannot do so because it is secret. And yet as we know, the functioning of the intelligence agencies is absolutely essential to this fight we now have and will be essential in the future. So the public cannot really get involved because of the nature of the information, so we are dependent in this area more than any other on congressional oversight. And that is why we made such a point in our report of saying how important we thought congressional oversight was.

In talking about it, we used the word "dysfunctional." Now, that was not our word. That word came from members of both parties on the Intelligence Committees.

Now, we made recommendations and Congress decided not to pursue those recommendations. But it is too important to just let it sit. It is too important that Congress' oversight be as good as it possibly can be.

When we interviewed this Secretary of Homeland Security, she made exactly the same point that her predecessors have made: That she has to report to 60 to 70 congressional committees and subcommittees and, therefore, spent almost one-third of her time and the time of her deputies in testifying in this complex system rather than working to actually improve our overall security in this country.

We also have suggested that perhaps the Intelligence Committees have more authority, particularly over the finances, so that they could do a better job and command the answers we need from the intelligence communities.

We point this out because we think it is so very important that congressional oversight ensures the intelligence community is operating effectively, and also, by the way, to help resolve disputes about conflicting roles and missions. So we would urge the Congress to look at this issue again and take action to strengthen the oversight capabilities of the Intelligence Committees.

Thank you very much.

Chairman LIEBERMAN. Thanks, Governor Kean. Let me begin just by saying "amen" to what you have just said. As you look back at the 9/11 Commission's recommendations and Congress' response to them, Congress was really quite effective at taking on some of the status quo, and notwithstanding the resistance of different elements of the intelligence community, the Department of Defense, existing agencies, we pushed through in the national interest to achieve the reforms we did. The one existing institution that Congress proved itself less willing to reform was Congress itself. So you are absolutely right. As you remember, Senator Collins and I tried on the floor a couple of times to adopt the reforms, we recommend the reforms that you have gone back to this morning, and in an uncharacteristic experience for us, we lost miserably.

But I want to challenge you, and I accept this challenge myself. Let us figure out with the families again if we can make another run at this, because it really is important and it does hamper the conduct of our homeland security and intelligence communities by those involved. And there is no excuse for it except turf protection, frankly. So I thank you for bringing that up, and let us come back to it.

Let me say that last winter we noted 5 years of the post-9/11 Commission Act, 5 years of the existence of the reforms. Senator Collins and I decided then actually to begin a 5-year oversight review this year, and then, unfortunately, it came after both the Fort Hood and the Christmas Day bombing. So we naturally begin this in the context of that.

But the fact is, as we try to pull back from those two events particularly—and we should not pull back all the way just for the moment—the reforms really worked to protect us. Maybe we had some good fortune, obviously good luck. But the truth is that there was not a successful terrorist attack really since September 11, 2001.

But then in 2009, it seemed to us that the pace of the attempted attacks against the United States picked up. There were at least 12 that are publicly known. There were some others that have been not been discussed in public. And most troubling, of course, is that three attempted attacks actually successfully breached our home-

land defenses: Carlos Bledsoe in Arkansas walked into an army recruiting office, killed an army recruiter just because he was an army recruiter; Major Hasan at Fort Hood; and then the attempt on Christmas Day.

So I wanted to ask either of you or both of you to step back a little bit and give us your best judgment about what is going on out there, what happened in 2009 to increase the pace of attacks against our homeland. Is it just, as you said, Congressman Hamilton, a loss of the sense of urgency here? Is something different going on that we in Congress and the Executive Branch need to respond to?

Mr. HAMILTON. Senator, I think the immediate thought I have in response to your question is that al-Qaeda has changed. The September 11, 2001, attack, as all of us know, was a highly sophisticated effort.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. It took a lot of planning. It took a lot of people. It did not take an awful lot of money, but it really was impressive from the standpoint of planning and execution. And I think the attacks that you referred to in 2009 have been largely solo performances.

Now, in some respects that probably indicates progress, and it means that our aggressive actions with regard to al-Qaeda have been successful, at least in part. And it is more difficult for al-Qaeda to organize the complicated attacks. But their intent remains, and perhaps their capabilities have been diminished.

I do not have any doubt at all that they are sitting there somewhere plotting how to get at us. And they are going to do it any way they can, with any capability that they have. And if they cannot organize an effort to fly airplanes into the World Trade tower, then they can get one person to get on an airplane and try to blow it apart. So our guard has to stay up.

Now, I think, second, that our defenses and our offenses with regard to the terrorist threat have improved. We are a lot better than we were. And that is no reason for patting ourselves on the back or complacency, but it is a fact. You have a lot of people in the government today who are very talented, and they are working very hard to block these attacks, not just the Federal Government but in city and State governments as well. We all know the efforts going forward in New York City, for example. So I think both factors are present.

Chairman LIEBERMAN. Governor Kean, do you want to add anything?

Mr. KEAN. Just a little bit. I think traditionally, at least, al-Qaeda used to talk about big things.

Chairman LIEBERMAN. Right.

Mr. KEAN. And after September 11, 2001, they talked even about doing something, if they could—Osama bin Laden himself talked about nuclear attach and what have you. The last big attack, I think, they seem to have attempted was that one in Britain where they were going to blow up the airliners.

It does say something that they have not succeeded in any of those things or not been able to pull them off, and now they are obviously saying, all right, in a sense, let us try the smaller stuff.

And for bin Laden himself, if that was bin Laden in that tape, to take credit for a failed bomber from Yemen, that is not all bad. It shows he has not much else to talk about at this point. But I suspect we are going to have to be aware that while they would still like to plan the big one, now they are going to let loose whatever they can because they want to show some success, I think, in our homeland.

Chairman LIEBERMAN. I appreciate that response. It gives us all something to think about. Let me just, in the time I have remaining, focus in a little bit on the DNI.

When we were having the legislative battles over creating the DNI, I think that a lot of us would have guessed that the toughest battles that the DNI would have, once created, would be with the defense intelligence community. In fact, that seems not to have happened, and if there have been battles internally, it has actually been within the intelligence community.

Though I think you raised reasonable questions in your testimony about whether the DNI has become too large, you also are very strong in saying that we gave them a lot to do. But, bottom line, I want to just draw from you what I assume from your statements is your position, that you have no second thoughts about creating the DNI. Am I right about that?

Mr. KEAN. Yes, absolutely right. We believe that the DNI is exactly what we need right now.

Chairman LIEBERMAN. And, second, that though you raised questions about the efficiency of spending money. I take it that when you are talking about clarifying mission, you are not talking about weakening the DNI.

Mr. HAMILTON. That is exactly right. We want to strengthen the DNI with regard to key authorities—budget, personnel, and other matters. We are not talking about weakening him in any way.

I must say, I saw an organizational chart of the DNI's office the other day. Perhaps you have seen it. I was quite surprised at things they have taken on. It is worth a quick glance if you have not seen it. And to ask the question, is this really necessary to be done by the DNI, and I think valid questions can be raised about some of those efforts.

For example, they have a university. I do not know what that is. I know what a university is, but in this context, I do not know what it is. And I am not sure that is the job of the DNI. But, anyway, I think all of that needs to be explored, but we have no second thoughts.

Look, this is a great big, sprawling, aggressive, massive, hugely funded enterprise, the intelligence community.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. And you have to have somebody at the top of it with authority, or it just is not going to work. Now, that authority obviously has to be accountable authority. But somebody has to knock heads together to get over this mind-set of "I can have the information, you cannot," and get outside the stovepipe and to force—I think the word is appropriate—the integration of the intelligence community. That authority should be given in the DNI. I think he cannot exercise it, no matter what the statute says, without very strong presidential backing.

Chairman LIEBERMAN. Well, I agree. I do not mean to ask an awkward question, but I will. Is it too early to evaluate President Obama's relationship with the DNI and whether that measure of leadership that you would like to see from the President has been seen thus far in this Administration?

Mr. HAMILTON. It is my impression that the intelligence community is relatively new to the President. I think he began to receive intelligence somewhere along the campaign. Senator McCain can tell you when that happens. And my impression is that his instincts are probably good, but he is still kind of feeling his way. His preference may be—he said, "I have appointed good people here," and he has done some good appointments, I think. But I do not think he has a firm grasp yet of the intelligence community, and, therefore, I am pretty strong in my thought that he has to step in pretty hard here, or some of these tensions which have surfaced will exacerbate.

Chairman LIEBERMAN. Thank you. My time is up. Senator Collins.

Senator COLLINS. Mr. Chairman, let me follow up on exactly the point that you just raised.

The law is clear on who is in charge of the intelligence community. I remember the debates we had and how difficult they were in establishing the quarterback, the one person who was going to be accountable. And yet in spite of what appears to be a very clear legal mandate, the DNI and the Director of the CIA still seem to be engaged in significant turf battles.

In just the past year alone, reports indicate that the White House has had to intervene in disputes over the CIA's role in Afghanistan, the chain of command over covert action, and the designation of the chief U.S. intelligence officer in overseas posts. Those conflicts undermine the unity of effort that was the goal that we shared and the very reason we created the DNI. And I am concerned by reports that the President may have inadvertently undermined the DNI by siding with the CIA in these disputes. So I have two questions for you.

First, does the President need to more clearly indicate to the intelligence community that the DNI is in charge and has his full support?

And, second, do you believe that the relationship needs to be further clarified in law? Or is this a matter of the law being adequate for the most part and the President needing to lay down the law, if you will? Governor Kean, we will start with you.

Mr. KEAN. Yes, I think we have always thought—and Mr. Hamilton has been very articulate in this over the years—that the success of the DNI is going to depend totally on the leadership of the President. He has to make it absolutely clear.

Now, in a way, this Christmas Day bomber did us a favor. I think we were not paying close attention to this, and it is understandable. We were talking about health care, cap-and-trade, certainly the economy, and we should have been. But we got distracted a bit. I think everybody from the President on down got distracted, and were not paying full attention to this area, and so these things were allowed to develop and cracks were allowed to form, and things got a little off track. Now I think we have a wake-

up call, and I think the President in his statements, in his news conferences, in this area has been clear. And I assume that the actions are going to follow the statements and that he is going to pay now strict attention to this problem, and no matter what else is going on, his leadership is going to be called for in this area, and I assume he is going to exercise it. But it is not going to happen without that. I mean, he has to stay on top of this. He has to make clear what he believes the authorities are, and where there is any kind of dispute, he has to step in right away. He cannot allow it to fester.

Senator COLLINS. Congressman Hamilton.

Mr. HAMILTON. My answer to your first question obviously is yes. I have tried to make that clear. The President does need very clearly to make it crystal clear to everybody in the intelligence community that the DNI is in charge.

As I said in my testimony, the exercise of that authority—but the DNI requires a lot of diplomacy and sensitivity. And that is a real challenge in how you exercise that leadership, but he should be in charge.

Now, do you need a change in the law? That is a little tougher. In the short term, it does not make any difference. You are not going to change this law. The threat is out there now. The flaws have been revealed. You have to deal with those flaws right now. You cannot wait to change the law. So it does not make any difference in the short term.

In the longer term, this is not the first law ever passed by the U.S. Congress that may have had some ambiguity in it. And it might very well be that you can refine it down the line. I do not have specific language to offer to you today, but I guess my central feeling is this is the law, it is going to be that way for a while, and you have to make it work.

Senator COLLINS. Thank you.

Last week I questioned the DNI, the head of the National Counterterrorism Center, and the Secretary of Homeland Security about whether they were consulted in the decision to charge Abdulmutallab as a criminal and give him his Miranda rights and give him a lawyer, which caused him to immediately stop cooperating and answering questions.

I was shocked to hear from each of these top officials that they were not consulted about a decision that had such implications for our Nation's ability to better understand what may be further plots emanating from Yemen.

Governor Kean, what was your reaction to learning that our Nation's top intelligence officials had not been consulted about that decision?

Mr. KEAN. I was shocked and I was upset. It made no sense whatsoever to me that here is a man who may have trained with other people who are trying to get into this country in one way or another; who may have worked with some of the top leadership in Yemen and al-Qaeda generally, and we do not know the details of that; who may know about other plots that are pending, and we have not found out about them.

This is not just about prosecuting an individual. This is protecting the American people. And decisions of this kind should

never be made without the full input of the greater intelligence community, particularly the DNI, but also the CIA, the FBI, and other members of the intelligence community. And the fact that this was done without that kind of consultation was to me upsetting and shocking. And, by the way, I come from the New York area. Regardless of how we feel about whether that trial should be going on in New York, again, I gather that the Attorney General did not consult any member of the intelligence community before making that decision, which also has security implications.

So I think we have to get our act together and recognize that we should not make any major decision like this without first consulting the members of the intelligence community. And I just do not believe this individual should have been given all these rights or the lawyers before he was questioned fully.

Senator COLLINS. Thank you. Congressman Hamilton.

Mr. Hamilton. Well, I agree with Governor Kean's comments. I think we have to be guided by the principle, and we need to get all the information we can out of these people. That is the principle.

Now, what concerned me in the answers that you referred to and the questions you put was there did not seem to be a policy of the government as to how to handle these people, and that has to be clarified. I am not surprised the FBI stepped in. They are there when the plane lands. They go in. But there has to be a policy. It has to be clarified.

Your legislation or your proposed bill, which, as I understand it, mandates consultation with the DNI——

Senator COLLINS. Yes.

Mr. HAMILTON [continuing]. Makes all kinds of sense to me. The Director of National Intelligence surely should be consulted, but, importantly, there must be a policy.

One of the things we learned in the 9/11 Commission Report, as we got into this question of interrogation, is that this is a difficult business, interrogating people, and you better be very sure that you have the right people asking the questions.

Now, we can have differences of opinion as to what kind of pressure ought to be put on a suspect. But interrogating people takes patience and it takes skill, and you have to train an interrogator very carefully.

I am attracted to the idea of a High-Value Interrogation Group (HIG). I do not think we have paid enough attention to the professionalism, if you would, of the interrogator. And I am not acquainted with the details of that, but I hope it is developing highly skilled people who know how to interrogate. An awful lot is at stake in finding out all you possibly can.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

I would just say briefly that one of the surprising sort of facts we learned afterward is that there was a recommendation and I thought an announcement at the beginning of a High-Value Interrogation Group. As a matter of fact, one of the witnesses last week referred to it by the initials HIG. We are going to ask this question, but as far as I can determine now, the group was never fully operational, never set up, so it was not in a position to be called on to

do exactly what we would have wanted it to do, as you both have said, after Mr. Abdulmutallab was apprehended. Thank you.

The remaining Senators will, as always, be called in order of appearance here at the hearing room, and it will be Senators Carper, McCain, Bennett, Kirk, Burris. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman. Again, gentlemen, welcome. It is great to see you again. Thank you for the wonderful work you continue to do for our country.

I am going to ask a question later in my allocated time that will draw on, I think, the great success and extraordinary leadership you provided for the 9/11 Commission to see what we can garner from that experience and as we prepare to move forward this week on legislation on a different commission, either a statutory commission that focuses on deficit reduction or perhaps a commission set up by an Executive Order. But I want to just bat some ideas around and just to ask for your thoughts given, I think, the extraordinary success that we realized under your leadership.

I like to say that the road to improvement is always under construction, and that is certainly through when it comes to finding ways to stop the bad guys from doing bad things to our country. When your Commission completed its work and made your recommendations to us, I know you made a large number of recommendations, dozens of recommendations. The number 40 sticks in my mind, but I am probably wrong. But do you recall how many recommendations you made to us? And I think they were pretty much all bipartisan and unanimous.

Mr. HAMILTON. About 70.

Senator CARPER. How many, 70?

Mr. HAMILTON. Seventy.

Senator CARPER. Yes. Do you recall roughly how many we adopted?

Mr. HAMILTON. We have calculated, Senator Carper, that 80 percent of the Commission recommendations have been adopted in whole or in part, and I think "in part" covers a lot of ground. But most of those—and about 20 percent—well, a little less than 20 percent outright rejected. Some may still be pending in one way or the other.

Senator CARPER. One of you said earlier in response, I think, to Senator Lieberman's questions, you mentioned it has been 8 years since September 11, 2001, every day terrorists are targeting us here and around the world trying to create mischief, create mayhem, and they have so far not had a whole lot of luck. They have had some luck, bad luck for us, but they have missed opportunities as well.

Something that we have done, something that you have recommended, something that we have adopted, something that has been implemented by the Executive Branch, is being pursued by our men and women all over the world, something is working. And that does not mean, as I think Congressman Hamilton said, that we sit back and rest on our laurels.

But when you look at what we have done, including the things that you have recommended that really seem to be working, what

really stands out for you? When you look at what you have recommended that we have passed, that has been implemented by the Executive Branch, that does not meet muster, maybe that is incomplete, gets an incomplete, what might that be? Again, what do you think is really working well, is important to keep up? And where are some areas that maybe we did not follow up and recommendations were made but have not been implemented well?

Mr. KEAN. Well, I will start. Obviously, the creation of the DNI under the congressional legislation with the NCTC was the heart of our recommendation to force information sharing because the lack of information sharing was one of the things we found that probably led to September 11, 2001, as much as anything else. And at least if we had shared information, there is a good possibility it might have been prevented. So that was key. That has been done, and we have talking about today how well it is functioning, and I am sure your Committee will continue to do that.

I mentioned two areas before where recommendations have not been implemented. One is the Civil Liberties Commission, and we think that is very important, and basically it does not exist because the President has not appointed its members. And, second, congressional oversight, and we still do not believe—and we hear again from bipartisan people on both sides of the aisle that they are not satisfied in the Intelligence Committee that they have the ability right now to do the kind of oversight this country needs. And that is deeply disturbing because if they are not doing any oversight, nobody is doing the oversight.

Senator CARPER. Right.

Mr. KEAN. And that cannot continue to exist in this kind of problem.

Those would be the three things I would mention. I could mention a number of others, but those would be most important, I think.

Senator CARPER. Thank you, Governor Kean. Congressman Hamilton.

Mr. HAMILTON. Well, Governor Kean is on the mark. On the plus side, I would think the recommendations we made with regard to the intelligence community, including the DNI and the NCTC and other aspects, I would judge them broadly successful, not completely but broadly successful.

I think a lot of the recommendations we made in the transportation sector, the watchlists can certainly be improved, but we recommended that. Better detection equipment, we recommended that. We have been a little disappointed in the slowness of the adoption of some of the detection—improvement of some of the detection mechanisms. Cargo screening and all those kinds of things I think are underway, taking a little more time probably than we wanted to, but basically have been approved.

We had a whole chapter in the book on the 9/11 Commission on foreign policy recommendations on the question of how do you deal with the Islamic world. That was not so much legislative recommendations as foreign policy recommendations. And I think we have a ways to go in implementing those because our relationship with the Islamic world is a huge foreign policy challenge, and will be for decades to come, in all likelihood.

I want to emphasize the Civil Liberties and Privacy Board. Look, you have the capability today of surveillance and intrusion into the lives of people that is incredible, what the government can learn about you today, and all of these fancy technological devices we have to intrude into private lives. And we all support it. We think that is necessary. But if you have an argument today in the bureaucracy between the security people and the civil liberties people, I will tell you who is going to win the argument. It will be the security people every time.

We picked up the paper the other day, and we found out the FBI had been violating the law for 5 or 6 years. And it was not ever called to the attention—the inspector general finally found it out. This was the FBI, which is supposed to be sensitive to these matters.

The point here is that you need somebody out here in the government that is checking everything that is done with regard to security and asking themselves, can it be done better with a little more respect for privacy and civil liberties?

We all know that privacy and civil liberties are going to be invaded. We understand that. You cannot walk through an airport without understanding it. But we have to, I think, have a group with robust powers to be a counterbalance to the argument for security. And so Governor Kean and I, and I think all of our Commissioners, were very solid on that point.

Mr. KEAN. Very strong on it in a very bipartisan sense.

Senator CARPER. Mr. Chairman, could I take just one more minute and go back to the other question I wanted to ask? When I look at commissions that have been extraordinarily successful, I go back to 1982 Commission on Social Security which Congressman Hamilton, Senator McCain, and I voted for—I had the opportunity to vote for after they made the recommendations, not binding recommendations but recommendations which I think have served us well.

We have before us this week the idea of a statutory commission that gives us recommendations that are binding unless there is some kind of override that exists. The proposal would say most of the commissioners would be sitting Members of Congress. Another approach would say, no, they could be folks like you who bring a world of experience to it. Just given the success of this commission, just give us a little bit of advice as we go forward this week on a different, equally important challenge.

Mr. HAMILTON. Pick a chairman like Governor Kean. [Laughter.]

Senator CARPER. But how about the vice chairman?

Mr. HAMILTON. Let me tell you the first thing Governor Kean said to me—he was chairman, I was vice chairman—we knew each other by reputation, but we did not know each other well. Governor Kean walks into the room, and he says, "Lee, we are going to make all of these decisions jointly. We will not hire anybody, we will not fire anybody, we will not make any decisions unless we do it together."

Mr. KEAN. Look, Mr. Hamilton often said one of the fortunate things we had going for us is we were, as I think he used to put it, "reformed politicians"?

Senator CARPER. I describe myself as "a recovering governor."

Mr. KEAN. There was nobody on the 9/11 Commission who had any interest in running for anything. Or I do not think anybody particularly was looking for an appointment of any kind. So our minds were clear in a sense. Our agenda was trying to protect the country. And that fact probably enabled us to get over the kind of partisan—we met at a terrible time. This was going into one of the most divisive presidential elections in our history. And we started off with a Republican sitting here and a Democrat sitting over there, and the first time I walked in, Democrats were sitting in one corner. He and I walked into the room, and basically said, "Break it up." And after that I said Republicans are going to sit next to Democrats and Democrats are going to sit next to Republicans. We are never going to meet again unless we have that kind of seating arrangement.

But it helps to have your mind clear of any other problems so you can concentrate on whatever the task is, and not to care very much, personally, try to do the right thing, and we figured, as a Commission, we would try to do the right thing, and that was our mantra. You know, we would argue about these things, and then somebody would say, "Well, what do the facts show? What is the right thing here?" And that was usually how we came out.

Chairman LIEBERMAN. Thanks, Governor Kean. That was very helpful.

Senator CARPER. It was. And thank you for being so generous with the time. Thank you both very much.

Chairman LIEBERMAN. I know you will thank Senator McCain, too, because he is next. Senator McCain.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. You are not welcome. [Laughter.]

I want to thank our witnesses for their continued service to the country; especially, I would like to again welcome the September 11, 2001, families, without whom the 9/11 Commission would never have come into being and these much needed reforms would never have been enacted.

Congressman Hamilton, I was struck when you said 80 percent of the recommendations probably had been enacted into law. On page 419 of the 9/11 Commission Report, it says, "Strengthen congressional oversight of intelligence and homeland security. 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."

It seems to me we have not implemented that very strong language contained in your report. Is that accurate?

Mr. HAMILTON. Unfortunate, you are totally correct.

Senator MCCAIN. Then it seems to me, Mr. Chairman, that we ought to go back at it, and we ought to keep going back at it until we shame our colleagues into being more concerned about national security than they are about turf. And so I hope at the next opportunity we will join and try to push the changes that have been recommended by the Commission. Would you say it is probably the most important failure of all the recommendations that you made?

Mr. HAMILTON. Yes.

Mr. KEAN. I would, and we were told, by the way, by Members of the Congress who were on our Commission, four Members of Congress, and they all said when we proposed this, "This will be the most difficult recommendation to get implemented." And we said, "Yes, but it is the right thing to do," and everybody agreed it was the right thing to do, so we went ahead.

Senator MCCAIN. Well, I will ask the September 11, 2001, families to go into battle again for us. [Laughter.]

If anybody can get it done, you all can. I thank you.

I was disturbed by the events—and some of it was revealed in the hearing that the Chairman and the Ranking Member held just a short time ago—the 50-minute interrogation, the decision to give the Christmas Day bomber Miranda rights and a civil trial. All accounts—and I only know press accounts; I have no classified information—were that this individual was talking, and then there was a pause, and when he woke up, he had a lawyer. And, understandably, the lawyer did what lawyers do. That is their job. So I am not blaming the lawyers.

But how we could have made a decision the way we did brings me to a larger issue, and that is the whole issue of the disposition of detainees—Guantanamo, the trials, and under what circumstances. And it seems to me that the overall policy is so—the word may be "incoherent," or certainly, "not coordinated," I guess is a kinder description—that we now have an ad hoc decision making process regarding the treatment of detainees.

We still have not resolved the issue of enemy combatants, which we cannot bring to trial because of insufficient evidence, but yet we know we cannot release them. We have learned that there is a certain percentage—it varies, 10, 15, or 20 percent—of detainees, depending on who you talk to, that are back in the fight, including some in leadership roles.

So does this information make the argument for Congress and the Administration, or Congress alone, to develop legislation that addresses all these amorphous areas of trials, of detention, and particularly in this issue, the treatment of enemy combatants that you cannot bring to trial but at the same time cannot release? For example, an annual review of these cases. But so far, none of these have been translated into a policy that Members of Congress understand.

So Senator Lieberman, Senator Graham, and I are working on legislation to try to address this very important issue, and we want to work with the Administration to prevent another situation such as the Christmas Day bomber. Furthermore, we also want to resolve the existing situation where enemy combatants are going to be tried in New York, which you have already expressed your opinions about; some are going to be tried in Guantanamo; some may be tried in other places.

Does this whole Christmas Day bomber issue focus the absolute requirement that we address this issue in a policymaking and perhaps a legislative manner?

Mr. HAMILTON. I very much agree with your conclusion. These people present a real challenge for us within our constitutional system. The problem is you have a detainee; you cannot prove a criminal charge against him, let us say. At the same time, he could kill

you. It does not fit in the American constitutional system, and we have not figure it out yet.

I think the most important thing you said was that you, Senator Lieberman, and Senator Graham are working on it. I am delighted to hear that. I did not know it.

I think we hear a lot about how government does not work very well today, how dysfunctional it is. This has been an area where the Legislative Branch and the Executive Branch have failed, flat-out failed. We have had this challenge now for a good part of a decade, or maybe more. Neither President Bush nor President Obama has dealt with it, and the Congress has not dealt with it. I think it is a very tough bill to draft.

The important characteristic that is needed in the bill, however the details are—and you have to look to lawyers who know a lot more about it than I do for the details. But the law has to be perceived as being fair, perceived by Americans as being fair, whatever that may mean; perceived by the foreign international community as being fair; and I think that is what you have to strive for. That does not mean you give them all the rights of an American citizen. I am not arguing that.

But, Senator, I applaud that initiative. I think this has been a failure of the U.S. Government as a whole to deal with this very tough problem, and I certainly wish you well on it.

Mr. KEAN. Senator, once again, thank you for your leadership. I could not agree with Mr. Hamilton more.

Senator MCCAIN. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator McCain. I appreciate your leadership on this. It has been very good to work with you and Senator Graham, and I think we are trying to make the point, and the witnesses have been very helpful, which is that the choice for our country in deciding how to deal with terrorism suspects we take into incarceration is not a choice between applying the rule of law and not applying the rule of law. We are a country of laws. It is a question of which rule of law. Is it the rule of domestic criminal law, or is it the rule of the laws of war? And, of course, I believe it is the second. That was a very important exchange. I thank you.

Senator Bennett, you are next.

OPENING STATEMENT OF SENATOR BENNETT

Senator BENNETT. Thank you very much, Mr. Chairman, I appreciate the dialogue, and I appreciate very much the witnesses and the important subjects you have discussed.

Rather than go back over some of those, because I think the record is now clear, Congressman Hamilton, let me pick up on a comment you made. It may appear to some to be a somewhat smaller issue, but you raised it—and I have an interest in it—when you talked about the necessity for better detection equipment.

I spend a lot of time going through airports, as do we all, but I have personally experienced higher technology with respect to body imaging. We have one of those on a trial basis at the Salt Lake City airport. I went through it without any bodily harm or any psychological embarrassment, no displays of any embarrassing fashion anywhere. And I am drafting language, planning to introduce

shortly legislation that would require Transportation Security Administration (TSA) to adopt and deploy advanced technology like the body imaging technology at an accelerated pace.

As you pointed out, it has been 8 years, and we are still using the old "mag and bag" technology, the magnetometer and searching the bags, which is not very effective, quite intrusive, and very slow. And I think we should get TSA to deploy technology with the capability to detect plastic explosives and liquid explosives, non-metallic threats and so on of this kind.

And, by the way, I very much support what TSA has done with respect to privacy in these technologies, and we need to make sure that we go as far as we can to see to it that is balanced as well.

We do that in the United States. Now, somebody gets on a plane in Yemen, transfers in Amsterdam. What kind of threat do we have in the world transportation network that says fine for TSA to be doing this, but it is not going to have any impact on the kind of thing that we saw in the form of the Christmas Day bomber. Give me your reaction to how technology can be used and how influential we can be in getting other countries to use it?

Mr. HAMILTON. I do not know anything that has frustrated me personally more than the inability over a period of years to develop adequate detection equipment. The most serious thing in my mind is the inability to detect nuclear materials, and I know we have spent a lot of money at that, and this is a problem that goes back well before September 11, 2001. But we still have not come up with it. And so I think there has to be a crash effort, if you will, in the research and development in the scientific community to develop better technology here.

The hijackers got on those planes on September 11, 2001, with 4-inch blade knives.

Senator BENNETT. Right.

Mr. HAMILTON. They knew you could not get on with 8-inch blades. These folks were very sophisticated about our vulnerabilities, and whenever we make a change, they begin to adapt to it. So the technology has to try to keep out in front.

I personally do not have any problem with the body images. I think they ought to be used. I am not dead sure they would have caught our December Day bomber and stopped that incident. In other words, people have said to me that even with body imaging, it might be he would have gotten through. But, in any case, they are clearly better than the metal detectors. Our adversaries here figured out a long time ago that they have to do something other than metal in order to cause problems.

Now, the international problem is a very difficult one, exceedingly difficult, and I know our people have spent a lot of time talking to other countries about strengthening their procedures. I think we have to get to the place where we do not let people into this country unless they have gone through a security process that is rigorous, however defined.

Senator BENNETT. Governor Kean.

Mr. KEAN. Our biggest defense now is not in technology in that area. It is technology in identifying people who are bad people, should not get visas, and should not get into this country anyway. And as you know, if you go to these centers, you can see every per-

son who is getting on a plane at that time heading for the United States, and little stars or whatever, if any of them are suspect in any way. That is probably, at the moment, the best defense we have. And, in fact, the Christmas Day bomber obviously should have been on those No Fly Lists if things had been done properly.

Having finished with that, I think I am for upgrading any technology we can, and recognizing that the people who are enemies, as Mr. Hamilton said, are going to try to upgrade their methods of getting through the technology at the same time we upgrade our technology as best they can. And so I think we should do that. But the best defense we have is still do not let the bad people get on the plane to begin with, do not let them get visas, do not let them get to the airport, and do not let them even approach getting on the plane to the United States.

Senator BENNETT. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Bennett.

Next we have Senator Kirk. It is possible that a vote will go off soon. Maybe it already has. When it does, I think I might go over and try to vote early and come back, but if I am not back when Senator Kirk finished, then, Senator Burris, why don't you go right ahead, because you are next.

OPENING STATEMENT OF SENATOR KIRK

Senator Kirk, thank you.

Senator KIRK. Thank you, Mr. Chairman. Thank you for your leadership and continuing oversight of this important matter we have addressed over time.

Let me thank our witnesses for their selfless and patriotic service throughout your public careers. It has been inspirational, I think, to all who know and have followed.

I also want to salute the families for their valor and persistence and recognize Carie Lemack, who worked closely with Senator Kennedy on help for the victims, and you folks deserve enormous praise and gratitude for your courage.

My question basically goes to this impression of almost information overload at NCTC. We have talked about and you quite rightly recognize the need to recruit and retain analysts of the highest talent and caliber and to recognize their prominence in this whole dilemma.

Do you have an impression that, given the amount of information, there are sufficient or adequate numbers of analysts of that caliber that are dealing with this?

Mr. KEAN. My information, frankly, is not recent enough to make that conclusion. I know last time I was deeply involved in this there was certainly not enough analysts, and certainly not enough good ones. And one of the problems I said was they were not promoted or recognized the same way, and we were not attracting the best people. I hope that has changed. I have no information. I just have not been into it one way or the other since that time.

Senator KIRK. Congressman Hamilton.

Mr. HAMILTON. Well, I agree with that. This is one of the things we in the National Security Preparedness Group, need to look at. As Governor Kean said in his testimony, he drove home the importance of the analysts, and that is absolutely correct. I do not really

know whether we have enough. I do not know whether the ones we have are sufficiently trained.

I do not think you produce an analyst quickly. I think it takes several years. And it is tough work. I mean, you are sitting there watching millions and millions of bytes of data come across the screen, and 99.9 percent of it is useless. And then there is the nugget in there. So you have to have not only first rate analysts, but you have to build into the system redundancy. I am not the least bit worried if you have two different agencies of the government doing similar work with regard to analyzing intelligence. But I think the question you have raised is really critical and needs to be followed up very carefully, and Congress needs to give full support to whatever the intelligence community needs to get top-flight analysts.

Senator KIRK. Thank you. Thank you both.

The other aspect of this analysis of our intelligence and the vast volume that we have is technology; this is apart from detection technology. This is about the technology that helps analysts synthesize, integrate, and read a pattern, if you will. Do you know or do you have an impression as to whether we really have the kind of state-of-the-art technology that allows us to do that and to share it with the various agencies of foreign responsibilities, the domestic responsibilities? Because it seems to me that the grid, if you will, or that state-of-the-art technology, combined with the kind of human resources you both talked about, is really the key to this whole puzzle.

Mr. HAMILTON. Absolutely. I very much agree with that, and I do not know the answer to the question, do we have the state-of-the-art technology? I have a suspicion we do not, but I may be in error. I hope I am.

In any event, what I do know is that we have to find the best people in this country on the question of data management. I mean, you are handling data—it has been cited several times here—in massive amounts, and you have to sort through that in order to have the best protection.

I do not know whether those people are in the government or in the private sector today, but wherever they are, we better find them and we better put them to use.

Senator KIRK. Anything to add, Governor Kean?

Mr. KEAN. That is absolutely correct. I remember when I was talking to President Clinton when we were doing the investigation, and he pointed out that our data management was so inferior in government compared to the data management in the private sector, and he mentioned credit card companies and he mentioned some other outfits that he had in Arkansas that he said could have identified these people right away. And we just did not have that technology at that point. I hope we are better at it. I just do not know.

Senator KIRK. Thank you very much. Thank you, Senator Collins, for my time.

Senator COLLINS [presiding]. Senator Burris.

OPENING STATEMENT OF SENATOR BURRIS

Senator BURRIS. Thank you, Madam Ranking Member. Gentlemen, I echo the comments of my colleagues in reference to your work. I was almost in your situation as a retired public official, but duty called and I am back. But you all indicated that you are not going back in it and you were able to do great work for the country, which we appreciate. And to the September 11, 2001, family members, I extend my heartfelt thanks to you for your persistence.

I have not been able to read your report. You know, as a new Senator, I am just going to have some general questions. I wonder, did you all take into consideration anything with reference to homegrown terrorists? I hear a lot about al-Qaeda and what will be coming from the foreign service. Did your Commission take into account homegrown actions?

Mr. HAMILTON. The 9/11 Commission did not because it really was not within our mandate. But since the 9/11 Commission and the development of the phenomenon of terrorism, it is quite clear that the homegrown or the lone-wolf terrorist has become a major threat and concern to the country. So, yes, in the National Security Preparedness Group, we certainly will be looking at that threat and seeing how we can improve our defenses against it. Not all of the bad guys, unfortunately, are from abroad. We have a few here.

Senator BURRIS. You are right, Congressman. Governor Kean, the same thing?

Mr. KEAN. I would simply agree with him.

Senator BURRIS. And, gentlemen, I just wonder, if we go back to the al-Qaeda situation now, what I tend to pick up there is that they are going to put chatter out through the various pipelines into all our security agencies that is misleading, misdirected, and you will never be able to tell what is really in fact a possible threat.

I understand that they are going to try to spend us into oblivion with costs, that they are going to have us try to come up with every contingency to try to protect ourselves, which is naturally going to impinge, Congressman, on the civil liberties that will be coming. And so you have these actions that are taking place, the chatter that is misleading, and the attempts to spend us into oblivion with all of these various ideas. They will come up with something so it is tit for tat, and that tat is going to tap us out eventually financially. Are there any comments on that, gentlemen?

Mr. HAMILTON. I think it has become quite clear that the approach that you are mentioning—in other words, trying to make us spend more and more by way of defense—is part of their strategy. And maybe even it is a successful part of their strategy. And maybe it is even one of the reasons they think they are winning in some areas.

The really dramatic example is September 11, 2001, itself. Governor Kean, what did we figure that cost?

Mr. KEAN. Huge.

Mr. HAMILTON. A very modest amount of money caused it, and just think of all the changes that have occurred in America since September 11, 2001. So, yes, but what your question raises for me, Senator, is one that does not ordinarily come into the debate on terrorism, and that is the question of cost-effectiveness. The security people can come up with an endless number of ideas as to

what you should do, and you really find it very difficult to argue against any of them because they have truth to them.

I think as we move along and as our costs continue to rise, the question you raise will become much more a part of the debate. Is it cost-effective?

Now, obviously, you want to err there on the side of security, and we clearly have. But I do not know what this country spends to fight terrorism today. I am not sure anybody has made a calculation of it. If they have, I have not seen it. But it is a huge amount of money, and so the cost-effectiveness question comes to the front.

Senator BURRIS. And, gentlemen, I have about 5 minutes to go and vote, so what we are going to do is to call a recess until Chairman Lieberman returns. Thank you.

[Recess.]

Chairman LIEBERMAN [presiding]. The hearing will come back to order. Thanks to the witnesses for putting up with this. I think probably my other colleagues are not going to return. If you have the patience, I will go one more round of questions. Then I will go back for a second vote.

You have really been extraordinarily helpful. Perhaps I should save my flattery until after I ask this round of questions. I will come back to it.

I want to talk just briefly with you about the National Counterterrorism Center, which we focused, understandably, more on the DNI and the general problem and some of the facts of the Christmas Day bombing. But, obviously, the 9/11 Commission Act created the NCTC "to serve 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." And an intelligence community directive designated NCTC as the mission manager, a literal term.

However, the report made to the President about the Christmas Day bombing states that there is analytic redundancy between the National Counterterrorism Center and the CIA. We referred to this a bit earlier, that responsibility was not designated to tracking threat streams from Yemen, and that analytical roles and responsibilities across the intelligence community need to be clarified.

In your testimony, as I have mentioned, you reinforce these points and note that "we need to do a better job of ensuring that someone within the intelligence community is designated as in charge of running down all leads with a particular threat stream."

Generally, what is your assessment of why counterterrorism analytical roles or analytic roles and responsibilities are unclear 5 years after the 9/11 Commission Act was adopted into law? Congressman Hamilton.

Mr. HAMILTON. Now, I am not sure I understand the question, Senator.

Chairman LIEBERMAN. Well, I guess it is a general question about looking back 5 years, because the law really put a charter in place. Why do you think that the analytic roles and responsibilities still seem to some extent to be unclear 5 years afterward?

Mr. HAMILTON. I think we simply do not yet realize the importance of the analyst in the system. If terrorism is the threat and if you have massive amounts of information coming to you, collec-

tion is one part of intelligence; analysis is the other part. The collection side we are very good at, the analyst side less good at. And I think the reason for it is because we simply have not given it the priority it deserves.

I am on a group that works with Director Mueller at the FBI, and he certainly has given great priority to counterterrorism. But in the FBI culture, the top man is the agent in charge, and if you are an FBI person, that is the job you have an ambition to achieve. And it is only in very recent years that they have begun to elevate the analyst to a comparable position as the agent in charge.

When you really think about it, the analyst drives what the FBI does. If their principal function is counterterrorism, the analyst has to drive the activity of the FBI. I do not think you have in the Federal civil service the incentives that you need, maybe we do not have the pay that we need to elevate the job of the analyst. I think it is a very tough job, and it takes a while for the Federal bureaucracy to respond to the need.

Chairman LIEBERMAN. Governor Kean, do you want to add anything to that?

Mr. KEAN. Yes, just also remember in this 5 years you are talking about—with the exception of the FBI, you had rotating people in every one of those positions.

Chairman LIEBERMAN. Right.

Mr. KEAN. When you passed the Act, I envisioned a DNI that would stay for a while. We have not had that, and I think we need that. We need somebody to focus, and some of these problems I think are unresolved simply because of a change in leadership.

Chairman LIEBERMAN. Yes. Is that something we should think of attempting to do by way of statutory amendment, to give the DNI a longer term? We actually argued this out during the legislative consideration of your Commission's work.

Mr. KEAN. Well, the first DNI left voluntarily. A term would not have kept him, I do not think.

Chairman LIEBERMAN. Right.

Mr. KEAN. So I think maybe the way to do it is rather through legislation or otherwise, have the understanding when somebody gets the job that, providing that you are doing the job well, we expect you to stay.

Mr. HAMILTON. It appeals to me, Senator. You have a 10-year term for the FBI Director.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. And Director of National Intelligence, it seems to me, is in a comparable position. Intelligence ought to be as removed from politics as possible. And so it makes sense to me.

Chairman LIEBERMAN. I am glad to hear that. I had not really thought about that going in, but that might be something to do to strengthen the DNI. And it has worked really pretty well overall with the FBI Director. We see it in this case with Bob Mueller who made a transition quite seamlessly between administrations.

Let me go back to the NCTC and ask if you would talk a little bit about what you think its role should be in relationship to other analysis organizations and to the so-called operators or intelligence collectors in the community. In other words, if I can borrow from what we were discussing earlier about the DNI, or should the Na-

tional Counterterrorism Center be the leader of the intelligence community's counterterrorism activities or just a coordinator?

Mr. HAMILTON. I think the analyst is the person who has to spot the problem and to spot the threat, and then there has to be an assignment of responsibility to someone to pursue vigorously that threat.

I do not think that is likely to be the analyst, but somebody has to be in charge. In other words, the analyst says we have five strands of information here that point to X as a threat. You cannot stop there. You have to pursue it. And somebody has to be assigned the responsibility of saying you go after X and make sure that X does not cause any problem.

I do not think that is the role of the NCTC. I am not quite sure where that responsibility lies, but the assignment of responsibility to investigate and to pursue a suspect has to be very clear.

You mentioned a moment ago the word "redundancy." I answered in response to Senator Kirk, I think it was, redundancy does not bother me particularly because if you have the CIA doing analytical work on the threat and the NCTC, that is OK, because the thing that impresses me about the analyst is the work can be boring, I mean really boring, sorting through massive amounts of data and trying to figure out what is right or what is significant. And somebody is going to be asleep at the switch now and then, so some redundancy does not bother me.

Chairman LIEBERMAN. Yes, I agree. This is a military concept, of course, both for personnel and for systems, in case one system breaks down. It is not a bad word to say that you have a redundant system. It is there to protect the life of the military person.

Governor Kean.

Mr. KEAN. I was just thinking one thing we ought to check on—I do not know the answer to this—is with these various agencies, who is attending the NCTC? What kind of priority are these agencies giving it? Are the people who are showing up people who are so junior in the line that if they come back with something, is it not going to be paid much attention to anyway? Are they sending some of their top people to the NCTC? Again, I do not know the answer. But that was one of the problems we had that we talked about a little bit at the time of the legislation, that these agencies have to give top priority and send their top people for the NCTC to be effective. And I do not know whether that is happening or not. I do not know the answer.

Chairman LIEBERMAN. It is a very good question. You know, we are going to follow up these two introductory hearings with a series of subject matter hearings, and we are going to do one on the NCTC, and that is a question we will ask. I probably said to both of you that when Senator Collins and I first went over to the NCTC after it was established in its new quarters, I remember that its then-Director took us around and said, "Look at this. This is where the CIA people sit. This is where the FBI people sit. And note there are no walls between them." So that was a big breakthrough. [Laughter.]

But now it is reasonable for us to ask exactly how they are working together, who are the people they are sending over, are they top-notch people. Of course, we all wanted, as you know, to make

sure that just as the military does, we would encourage jointness and reward it in career paths. In other words, if you are in the FBI and you are sent for a term over at the NCTC, it should be something good for your career, not something bad.

The 9/11 Commission Act also gave NCTC the authority to conduct "strategic operational planning for counterterrorism activities." The memories I have of the arguments over that particular provision and the fear could fill a book. But insofar as you know, I wanted to ask you—we are going to focus on this in one of our hearings. What is your assessment of how these authorities have been used by NCTC up until this time?

Mr. HAMILTON. My assessment, Senator, is that the intelligence community is overwhelmed by the tactical needs. In other words, you have a large number of military commanders out here who want intelligence on the enemy.

Chairman LIEBERMAN. Right.

Mr. HAMILTON. We are pretty good at getting that information. Or you have a diplomat who wants to sit down and talk with their counterpart in another country on whatever. We are pretty good at giving that diplomat information. Where we are less good, it seems to me, in the intelligence community is just the question you are raising, longer-term thinking.

Yemen probably is a pretty good example of it. We were behind the curve on Yemen. We simply did not realize how advanced they were in terms of striking the United States. But we need to have a significant element of the intelligence community thinking 5 years, 10 years ahead as to where the threats will come from. And that is even a tougher job, I guess, than the imminent threat. But it is very important that the United States not be surprised by these developments to the extent that you can possibly avoid it.

So I look upon our intelligence community as being very good, but if there is a weak spot, I think it tends to be in longer-term matters.

Chairman LIEBERMAN. Well said. Governor Kean.

Mr. KEAN. I would agree with that.

Chairman LIEBERMAN. Well, that is it, and I thank you very much for your time. What I was going to say before, thinking while walking over and back, that I remember a former Secretary of State once aroused a lot of interest when she said America is the indispensable Nation in the world. I say by way of compliment and warning that I fear that the two of you have made yourselves indispensable. It is really quite an extraordinary act of service you have performed, and all the more important in this particular moment in our political and governmental history that you have formed such a collaboration in which—it is not just bipartisan. It is nonpartisan. I do not think either one of you think about your party label when you do the work you are doing because you know how important it is to the national interest. And as a result, it continues to make you very important and influential.

Your testimony today has been very substantive. I do not want to make you feel too mature if I say I felt it was actually wise and very helpful to the Committee. So I thank you for it.

As I said, Senator Collins and I want to go to a series of subject matter hearings, and I would like to invite you and your staff at

the National Security Preparedness Group, that we consult with you about the directions in which we are going, and we would welcome your advice. But I honestly cannot thank you enough, and this has been a very constructive hearing for us.

We will keep the record of the hearing open for 15 days for any additional questions and statements. With that, I thank you and the hearing is adjourned.

[Whereupon, at 12 noon, the Committee was adjourned.]

THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: WATCHLISTING AND PRE-SCREENING

WEDNESDAY, MARCH 10, 2010

U.S. 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, Carper, Burris, Collins, and Brown.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Good morning and welcome to everyone.

Let me first express my pleasure at welcoming to this Committee as a Member, and attending a hearing for the first time, our colleague from Massachusetts, Senator Scott Brown. This is a Committee that Senator Collins and I have been on for some years now. We are proud of what we have been able to do. It is, as you know, a very bipartisan Committee and I think that is part of why we have been able to accomplish a lot over the years. I would say with particular regard to this Committee, it is very hospitable to independent-minded Senators. [Laughter.]

Senator COLLINS. From New England.

Chairman LIEBERMAN. From New England. [Laughter.]

Welcome. It is a pleasure.

This is the Committee's third hearing in a series that Senator Collins and I have begun to examine the extensive reforms made to our intelligence systems both after September 11, 2001, but particularly at the 5-year point from the enactment of the 9/11 Commission reforms.

Our goals here are to review where we have been, and how we are doing, to identify weaknesses that remain in the system and to make recommendations for administrative reform or legislation that are needed to correct those weaknesses.

Of course, these hearings have taken on added significance in the aftermath of the Christmas Day attempted terrorist attack in which Umar Farouk Abdulmutallab unfortunately exposed some serious weaknesses in our Nation's homeland defenses.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00089 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

The last two hearings that we have done in this series gave us a broad overview of the human mistakes and systemic or structural shortcomings that contributed to the Christmas Day attack. Today, we are going to look at two of the most important components of our government's efforts to deny terrorists the ability to travel to the United States, and that is the creation and use of terrorism watchlists and the passenger pre-screening mechanisms that use these lists to identify potentially dangerous individuals and if, in fact, we determine they are such, to stop them from getting on airplanes coming to the United States.

On Christmas Day, our government was unable to pull together all the intelligence in its possession to stop Abdulmutallab before he got on that plane. This was not a failure to collect information. And unlike the missteps leading up to September 11, 2001, it was not a failure to share it. We knew that Abdulmutallab's father had concerns about his son's growing extremism and presence in Yemen. We had separate intelligence that there was a Nigerian—unnamed, unidentified, but a Nigerian nonetheless—training in Yemen with al-Qaeda on the Arabian Peninsula (AQAP). We heard separately of plans for a Christmas Day, or Christmas-time, attack on the United States. And again, separately, we knew of a reported telephone intercept that identified a man named Umar Farouk, without his last name, as a terrorist.

All those dots, so to speak, were on the same table, but our government was unable to connect them, in that sense, to separate this information out of the enormous mass of information our government collects and shares so that this terrorist could be stopped before he acted. We were just plain lucky, as we have said over and over again, that the device he had on him did not effectively explode on that plane.

In our first hearing, the Director of the National Counterterrorism Center (NCTC), Mike Leiter, acknowledged that the Center's information collection and sharing systems need to be smarter, as he put it, and I would add that in an era when Google, for instance, can aggregate information for anybody who goes on Google from scores of Web sites and databases throughout the world very quickly, it is just unacceptable that NCTC does not have the same ability to search and aggregate information across our government's intelligence databases.

I think we also need automated mechanisms to connect disparate data points 24/7, 365 days a year, and flag potential threats for analysts to examine. These systems are widely used in the private sector and need to be adopted by our intelligence community as soon as possible with our help.

The Abdulmutallab case also exposed weaknesses, I think, in our watchlisting system. Our intelligence agencies obviously need to view some of the tips or finger pointing that is sent them, given to our government, with skepticism. The fact is that some informants may be motivated by spite or rivalry. But most are not, and it is just unacceptable, in this case, that Abdulmutallab's father—not just his father, but a respected business leader in Nigeria—was not considered a credible enough source for his information to have put his son on the watchlist without corroborating evidence. So I hope to hear from our witnesses today how the watchlisting process

has been modified to ensure that this kind of error will not be made again.

Another watchlisting problem, I think, concerns the screening of individuals on the watchlist who are not U.S. citizens or permanent residents. We are historically one of the most welcoming countries in the world to visitors and legal immigrants. But travel to the United States is a privilege, not a right. In my opinion, if the government concludes that there is any reason to believe that someone may have ties to terrorist activities, that person should be required to undergo secondary physical screening, at least, before being allowed to board a plane bound for the United States of America.

And finally, we need to dramatically expand our ability to prescreen travelers, both internationally and domestically. Right now, the government only begins to receive important identifying information about international travelers when they check in for their flight. In fact, most of this information is conveyed to the Department of Homeland Security (DHS) only after an airplane's doors close, or are about to close, which obviously makes it practically impossible for DHS to fully vet passengers before a plane takes off. In fact, that was the case on Christmas Day, and it argues loudly that we must find a way to start in-depth vetting in advance of a passenger's arrival at the airport using modern information gathering technology.

We need to ensure, I think, that the DHS has the identifying information it needs about international passengers at least 24 hours before departure and that it fully implements Secure Flight procedures to ensure that all passengers on all flights are systematically checked against the terrorism watchlist.

So this hearing is, in our opinion, an important opportunity to examine the next steps we need to take to continue to strengthen these watchlists and pre-screening systems that have been adopted after September 11, 2001, and particularly after the passage of the 9/11 Commission legislation.

The fact is, we are doing much better at this than we did on September 11, 2001, but what the Christmas Day bombing attempt shows is that we have to do better yet to ensure that the next Abdulmutallab is not allowed to get on a plane to the United States.

We have a very good group of witnesses before the Committee today. I want to say to you before we call on you that I think you have some of the toughest jobs in the U.S. Government, and therefore, you are subjected to disappointment or criticism periodically. I want to thank you for your commitment and service to our country.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Let me start by joining you in welcoming Senator Brown to our Committee. We are delighted to have you, Senator, join this great Committee. I think you will enjoy it very much.

I understand on the other side of the aisle we are also going to be gaining a member. A second Delaware Senator, I believe, is coming our way.

Chairman LIEBERMAN. This is true. I am tempted to make a joke about Senator Carper, but I think it will only get me in trouble.

Senator COLLINS. I thought I was giving you a good opportunity.

Chairman LIEBERMAN. Yes. I was going to say that one is enough—— [Laughter.]

But Senator Kaufman will be a great addition to this Committee, and along with Senator Brown, really strengthens our membership.

Senator COLLINS. Thank you.

Today's hearing focuses on two fundamental questions. Why was the Christmas Day bomber allowed to travel to the United States? And why was his name not included on the terrorist watchlist?

We know, as the Chairman has pointed out, that Abdulmutallab's father had informed the American Embassy in Nigeria of his Islamist extremist connections in Yemen more than a month before he boarded the flight to Detroit. We also know that his name was included in the broadest terrorist database known as the Terrorist Identities Datamart Environment (TIDE). But despite this alarming information, the system failed to bar Abdulmutallab from boarding Flight 253 to America.

As I look at this case, over and over again, I see missed opportunities. From my perspective, the State Department clearly had sufficient information to revoke Abdulmutallab's visa. State Department officials already had decided to question him about his ties to extremists if he chose to renew his visa.

It is baffling to me that Abdulmutallab could have been considered a threat to the United States in the future based on his extremist ties but not a sufficient current threat to suspend his visa. That defies both logic and common sense. Had the State Department taken the action to revoke or suspend his visa, it would have prevented him from traveling to our country, a missed opportunity.

Another missed opportunity occurred in Amsterdam. Amsterdam is one of those rare airports in Europe and throughout the world where a small number of U.S. immigration advisory officials are stationed. These officers can ask an airline not to board a passenger who will be prohibited from entering our country upon arrival. They receive a list of passengers of concern, including those whose visas have been revoked or flagged by the State Department. This was another missed opportunity to stop Abdulmutallab.

Another missed opportunity to stop him apparently occurred at the National Counterterrorism Center. The President has stated that there was ample intelligence on Abdulmutallab to warrant his inclusion on the No Fly List, yet this did not occur even after his father's warning. It did not occur because other streams of intelligence mentioned by the Chairman were not connected until it was too late.

A basic question about this missed opportunity is why did the intelligence community fail to analyze all the available information related to Abdulmutallab? Some intelligence experts tell me that outmoded computer systems are a factor. Despite the vast improvements in information sharing since 2001, and particularly since the bill that we authored in 2004, our intelligence community continues to rely on internal systems and processes that are relics from the days before the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). These outdated systems apparently

do not effectively surface intelligence information so that analysts and security officials can identify threats in real time.

I would like to know what the Administration's plans are for upgrading these systems to allow for more effective searching of terrorist information, for Google-izing, if you will, information across the government. For starters, identifying individuals in the terrorist databases who have valid U.S. visas should not be that complicated a task.

We must also examine how we can better identify individuals who should be on watchlists for additional screening at airports. For example, we know that Abdulmutallab was identified for additional screening, but only once he arrived in Detroit. This identification, as the Chairman has pointed out, was done while the flight was in the air or just after the door had closed. Why was that same information not used to identify him earlier, before he boarded his flight, for additional screening and an interview, as well? Another missed opportunity.

As this case demonstrates, waiting until a suspect terrorist arrives in our country to conduct additional screening is waiting too long, another missed opportunity.

We must continue to strengthen our watchlisting and screening systems, including evaluating the standards that are now used to include an individual on watchlists and look at which standards are used for which watchlists and whether they need to be strengthened, as I think is evident.

The bottom line is, until these systems work more effectively, work more seamlessly, we will not be able to prevent terrorists from traveling to our Nation.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

Senator Brown, it is our custom just to have Senator Collins and me make an opening statement. If you have anything you would like to say here at the outset, I would be happy to give you the time.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. Thank you very much. I would just like to thank you for your warm welcome. Obviously, I have worked closely with both of you, and obviously, Senator Burris, as well. I want to say that I am honored to be on this Committee, having served, and still serving in the military for 30 years, it is something I think about every single day. So I am hoping that I can add a little bit to what you are doing and I look forward to serving. Thank you.

Chairman LIEBERMAN. Thank you. I am sure you will add a lot.

Let us go to our witnesses now. We will begin with Russell Travers, Deputy Director for Information Sharing and Knowledge Development at the National Counterterrorism Center, Office of the Director of National Intelligence. The National Counterterrorism Center is probably one of the least known, most important agencies in our government. We are very proud of its establishment in the 9/11 Commission legislation and the work that it has done since then to protect our homeland security.

Thank you, Mr. Travers. We welcome your testimony now.

TESTIMONY OF RUSSELL E. TRAVERS,[1] DEPUTY DIRECTOR, INFORMATION SHARING AND KNOWLEDGE DEVELOPMENT, NATIONAL COUNTERTERRORISM CENTER, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. TRAVERS. Thank you, Mr. Chairman, Senator Collins, and Members of the Committee. It is certainly a pleasure to be here to talk about NCTC's role in the process of screening.

I would like to first build on your opening comments and drill down a little bit. I want to put you in the shoes of terrorist identities analysts to give you a sense of the three main challenges that we confront every day.

Challenge one, you have already alluded to. It is, in fact, the quantity and quality of information that comes in every day, literally terabytes, sometimes petabytes of information that come in, sometimes described as vastly exceeding the holdings of the Library of Congress. It is an immense amount of information. And, of course, we have many tools that will sort and sift and cull and highlight those billions of electrons that come into the community. In the case of NCTC, we do have 30 or so networks that come in, bringing in terrorist identities information, and we net that down every day to many thousands of individual intelligence reports dealing with terrorism.

The important point with respect to watchlisting is that every day, approximately, plus or minus, 10,000 names are coming into the terrorist identities analytic community.

Our 24-hour operations center certainly helps to net that information further down. I will just give you a sense of what they do. The size of my morning read book on Monday morning when I walk in, is 842 pages, 1,520 pieces of information. And we further will net that down and have daily video teleconferences with the Committee, and what we try to do is to discuss the two or three dozen highest-level threat scenarios that are ongoing at the time. We will have situation reports. We have a daily threat matrix and so forth and video teleconferencing across the center. And with the community, Abdulmutallab never made any of that discussion. He was literally down in the noise, and that is an issue that we need to confront.

Related to the quantity of material is the issue of quality, and here I would fall back on the rather overused metaphor of dot connecting, I think. If you do envision a huge field of dots, many have something to do with terrorism for sure, generally fragmentary, often ambiguous, but a large percentage are simply wrong, some combination of circular reporting, poison pens, mistaken identities, lies, and so forth, and that can be kind of difficult for us to distinguish. So that is challenge one.

The second major challenge you would confront—remember those 10,000 names I talked about. If we are dealing with Sunni extremism, then they are Arabic names. And now you have to get past a Western convention of first, middle, and last. Instead, you are dealing with patronymics, ethnic and tribal affiliations, and honorifics. Different names will be used for different purposes. It is complex, even assuming that they do not want to hide their iden-

[1] The prepared statement of Mr. Travers appears in the Appendix on page 306.

tity. The September 11, 2001, hijackers, as you remember, used 362 name variations.

A more recent case, Abu Musab al-Zarkawi, the former, now deceased leader of al-Qaeda in Iraq, had 60-some aliases that we knew of, and then each one of those names could be spelled in upwards of 100 different ways.

Commonality of names, also a problem. Let us assume that we have good intelligence that one Mohammed al-Shammari is a terrorist. I asked one of my Arab linguists to take a look at a Middle Eastern phone book, 500,000 names. There were 480 exact matches for that name, and that, of course, is a big issue when it comes to false positives.

And we often get partial names. Abu Mohammed from Peshawar is a terrorist. That is the functional equivalent of saying that the father of John from Boston is a terrorist. It is a huge problem for us.

And that brings me to the third challenge. What exactly is a terrorist? He swears loyalty to bin Laden. He attacks U.S. interests. He went to a camp in the Federally Administered Tribal Areas (FATA). Those are easy. What if he is an associate of a terrorist or an affiliate? What if he just gave money to an extremist cause? Those are a little grayer. What if he gave money to a non-governmental organization (NGO)? That NGO supports legitimate and extremist causes. What if he owns a bookstore that sells mainly extremist literature? What if he is in a chat room or on a web forum espousing "extremist rhetoric"? What if he is under the influence of extremists and he goes off to practice not jihad, but dawa, proselytizing? They get very gray in a hurry.

The point is, we go from very easy cases to very hard. They are, in fact, gray areas, and that gets to the issue of standards that Senator Collins talked about and that is one of the issues that the community is working its way through.

Mr. Chairman, none of this is intended as an excuse. As Mike Leiter said, we are endeavoring very hard to do better. The analytic and watchlisting communities are, in fact, working hard to improve on the gaps that were identified on December 25, 2009.

At the President's direction, NCTC is focused on improving the capability we have to pursue fragmentary information as well as to enhance TIDE records. And that builds on the business processes and technical enhancements that have been ongoing at NCTC for many years.

I would, however, caution against the belief that there is any silver technical bullet. We utilize a lot of tools and search capabilities and we have looked at many, many more. Because of the challenges I alluded to before, notions of a Google-like search or a federated search are actually of relatively limited value. We have significant Google-like searches that will go across many message-handling systems and we still would not have come across Umar Farouk.

Frankly, the further you move in the direction of commingling foreign and domestic data in a single enclave where you can effectively apply tools, the harder the legal, policy, and privacy issues become, and perhaps we can talk about that in the question and answer rounds.

In closing, let me just reinforce a couple of points from my prepared statement. First, it is important to highlight what December 25 was not. I agree with you entirely. It does not in any way call into question the basic watchlisting architecture that was set up by Homeland Security Presidential Directive 6. In NCTC's view, the basic plumbing is right. We can, in fact, pass the right information to the right organizations. Standards and procedures, they are being looked at. From our perspective, there could be significant resource implications. We can talk about that.

Nor is December 25 about information sharing. We certainly have some hard information sharing issues, as I suggested, but in this case, virtually every analyst within the intelligence community had access to the two pieces of key information to which you alluded. Rather, December 25 highlights a longstanding and very difficult problem, and that is how you identify and integrate fragmentary information when nothing is blinking bright red. That is the key challenge for us and we look forward to discussing how NCTC is addressing those in the question and answer rounds.

Chairman LIEBERMAN. Thanks, Mr. Travers. You actually raise a number of provocative questions which we will look forward to discussing with you.

Timothy Healy is the Director of the Terrorist Screening Center (TSC), which is located in the Federal Bureau of Investigation at the Department of Justice. Mr. Healy, we thank you for returning to the Committee and welcome your testimony now.

TESTIMONY OF TIMOTHY J. HEALY,[1] DIRECTOR, TERRORIST SCREENING CENTER, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. HEALY. Thank you, sir. Chairman Lieberman, Ranking Member Collins, Senator Brown, and Senator Burris, thank you for the opportunity to talk about the Terrorist Screening Center and our role in the interagency watchlisting process.

The attempted terrorist attack of Northwest 253 on December 25 highlights the ever-present terrorist threat to our homeland. Over the past 7 years, the TSC has played a vital role in a fight against terrorism by integrating terrorist information from law enforcement and intelligence communities into a single database known as the Terrorist Screening Center Database (TSDB), or the terrorist watchlist. This watchlist populates various screening systems used by the government.

Following the Christmas Day attack, or attempted attack, intense scrutiny has been placed on the requirements to nominate individuals to the watchlist, particularly the No Fly or Selectee List, which are subsets of the TSDB. This requirement or standard has evolved over time based on the experience of the watchlisting community and the issuance of additional presidential directives. Throughout this process, the TSC has remained committed to protecting the American public while simultaneously protecting privacy and civil liberties. As our efforts continue to evolve in response to the new threat and intelligence, your support has been outstanding and it is necessary in our continued successful mission.

[1] The prepared statement of Mr. Healy appears in the Appendix on page 310.

Let me begin by telling you about the watchlisting process, but before that, the watchlisting process for the TSC is about half our job. The other half is how we handle encounters when we do encounter the terrorist subject and that coordinated law enforcement or operational response.

But for the watchlisting nomination process, it can be best described as a watchlisting enterprise because it is a constant collaboration between the intelligence community, the National Counterterrorism Center, the FBI, and the TSC. NCTC relies upon information that is provided by the intelligence and law enforcement communities. The TSC relies on NCTC to do the analytical work and provide the accurate, credible information that we forward to our screeners. The screening community relies upon the TSC to make sure that the information is efficiently disseminated to their systems.

Once a known or suspected terrorist has been identified and included into TSDB, the TSC ensures the timely dissemination of that information to our screening partners. The utility of the watchlisting process is only effective when it is efficiently disseminated to those partners. The TSC has subject matter experts composed from experienced analysts from designated agencies that review the nominations to determine if they meet inclusion into the screening process.

There are four major U.S. Government systems that are supported by the TSC and the TSDB: (1) The Department of State's Consular Lookout and Support System (CLASS), is used for passport and visa applications. (2) Department of Homeland Security Traveler Enforcement Compliance System (TECS) is used for border and port entry systems. (3) The No Fly and Selectee Lists are used by the Transportation Security Administration for air passenger screening. (4) And the FBI's National Crime Information Center is used for domestic law enforcement encounters. The criteria for inclusion into each one of these systems is tailored by the mission, the legal authorities, and the information technology requirements and limitations of those systems.

Before December 25, 2009, the TSC had not received the nomination for Umar Farouk Abdulmutallab, and as a result, he was not watchlisted, as you have mentioned. Following the attempted terrorist attack, the President has initiated a review of why Umar Farouk Abdulmutallab was able to board on Northwest Flight 253.

As a result, the TSC was given two instructions. The first was to conduct a review in the TSDB of any individual within the TSDB that had a visa, beginning with the No Fly List and all the way down. That process has been completed.

The second was to develop recommendations on whether adjustments are needed to the watchlisting nomination guidance, including biographical or derogatory criteria, for inclusion into TIDE and TSDB, as well as the No Fly and Selectee Lists. To do so, the TSC convened its Policy Working Group, which consists of representatives from the National Counterterrorism Center, Central Intelligence Agency, National Security Agency, the Federal Bureau of Investigation, Department of Homeland Security, Department of Defense, Department of Justice, and Department of State to achieve this interagency consensus. That process is underway and

the TSC is working with the interagency partners to develop recommendations for consideration to the President.

At the direction of the White House and in conjunction with NCTC, the TSC has made some temporary and limited additions to the watchlist to counter the very specific threat that was observed on Christmas Day. As a result, the threat-related target group was identified and individuals from specific high-threat countries already residing in TIDE and TSDB were added to No Fly and Selectee Lists or upgraded into TSDB.

The TSC remains focused on fulfilling the presidential and interagency mandates to share terrorist screening information with our domestic and foreign partners. We have a standing commitment to improve our operational processes, to enhance our human capital, to increase our technical capabilities, and to continue to protect Americans from terrorist threats while protecting civil liberties and protecting privacy issues.

The TSC and the terrorist watchlisting has been a vital tool in the counterterrorism effort in the United States and will continue to do so.

Chairman Lieberman, Ranking Member Collins, I look forward to any questions that you may have.

Chairman LIEBERMAN. Thanks, Mr. Healy. I appreciate it.

Next, we will go on to Gale Rossides, Acting Administrator, Transportation Security Administration (TSA), at the Department of Homeland Security. Thanks for the work you have been doing as the Acting Administrator. As you know, the President made a nomination which will come before this Committee and the Commerce Committee to be Administrator and we hope to move that as quickly as possible. But we appreciate your excellent work in the interim.

TESTIMONY OF GALE D. ROSSIDES,[1] ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. ROSSIDES. Thank you, Mr. Chairman. Good morning, Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. I thank you for the opportunity to appear today to testify on behalf of the Transportation Security Administration.

I would like to begin by saying that TSA's core mission is one of counterterrorism. We continue the work we began 8 years ago with the establishment of TSA to close vulnerabilities with new technology and new processes in a complex aviation security regime. TSA operates in a high-threat environment day in and day out, which drives our officers and ourselves to be ever vigilant.

The attempted attack on Northwest Flight 253 on Christmas Day was a stark reminder that there are still those intent to do us harm. As we continue to harden elements of the system, we know that terrorists will look for gaps or exceptions they can exploit. The unthinkable is an opportunity for them.

Looking at the device used on December 25, it was very cleverly constructed, and it was intentionally hidden in a very sensitive

[1] The prepared statement of Ms. Rossides appears in the Appendix on page 316.

part of the individual's body to avert detection. We know that terrorists are studying our security measures and will exploit our social norms to their advantage. The men and women of TSA live with that threat every day.

The threat of an improvised explosive device (IED), getting onto an airplane is a significant focus for us. In 2006, we overhauled the training of our Transportation Security Officers to focus on finding IEDs. In 2007, we used proven science to train and deploy our first Behavior Detection Officers to identify people with hostile intent and refer them for additional screening.

We also began testing advanced imaging technology in 2007 to detect both metallic and non-metallic threats hidden on the body. TSA developed the requirements for this technology with the Transportation Security Lab at DHS and with the private sector. Because of the nearly 3 years of work we have already put into this, we currently have 43 machines already in place at 20 airports, and we will field approximately 500 units systemwide by the end of this calendar year.

Because IEDs can be hidden both on the body and in bags, we have also deployed bottled liquid scanners, advanced technology X-ray, and explosives trace detection units to enhance our officers' capability to find explosives. The U.S. Government is actually the world leader in testing and deploying these technologies. We are working with the national labs and the private sector to push the detection capabilities to even greater degrees, and we will continuously test and train our personnel. We are also sharing information with our international partners to assist other nations in raising their levels of security.

We are giving this mission every ounce of our energy. We continue to employ our layered approach to security to deter, disrupt, and stop attacks. What we are facing is not one man on one plane, we are facing a patient enemy who is determined to attack U.S. assets and the U.S. homeland.

Beyond the 450 U.S. airports, TSA also works with our international partners to secure the entire global aviation network. Because TSA does not conduct the actual screening overseas, we instead rely upon foreign governments, airport authorities, and carriers to conduct such screening. TSA does conduct inspection of foreign airports with the last points of departure for flights inbound to the United States. These inspections are to the standards set by the International Civil Aviation Organization (ICAO). TSA also imposes additional screening measures for all carriers flying into the United States.

Both before and after the Christmas Day incident, we have enjoyed a very strong working relationship with air carriers, foreign and domestic, and we greatly appreciate their commitment to keeping air travel safe. It is a testament to the strength of that relationship that on December 25, 2009, within 5 hours of TSA issuing new security directives to increase screening of passengers coming to the United States, 95 percent of our foreign partners were in compliance.

One of the key tools we have to keep known terrorists off of airplanes is Secure Flight. I am pleased to say that many large car-

riers are now participating, with the rest scheduled to be onboard by the end of this calendar year.

Chairman LIEBERMAN. Why don't you do us a favor and just take a moment and describe Secure Flight for the record and for those who are watching or listening.

Ms. ROSSIDES. Yes, sir. Once Secure Flight is operational, it will actually vet all of the passengers booked on every flight 72 hours in advance of the flight. That will actually give both TSA and our law enforcement, airport, and air carrier officials 72 hours to determine and further inspect somebody who shows up that would be of interest, either somebody who shows up as a No Fly or a Selectee.

The program is also going to help with passengers who have false positive matches, where they have the same name, because the system will actually vet using additional data elements, including the date of birth, a passport number, and a redress number if the passenger has filed for redress. That will ensure that passengers who are actually cleared will no longer have difficulty printing boarding passes. It will also provide much greater consistency, because today, the air carriers vet against the No Fly and Selectee Lists, and once Secure Flight is fully operational, TSA will do that vetting, which should give us a higher quality of the vetting.

TSA is an end user of the No Fly and Selectee Lists, and we will continue to work very closely with our law enforcement and intelligence partners to improve the information sharing efforts. Our mission requires us to continuously challenge ourselves, and we are dependent upon the cooperation and participation of stakeholders and passengers in order to keep this complex aviation system secure. We are extraordinarily grateful to the support of our partners at all levels of government, industry representatives, our international partners, the private sector, and especially the traveling public.

I would like to express my appreciation for this Committee's support of TSA and our programs, and I am particularly honored to serve alongside the everyday heroes in TSA. I am happy to answer your questions.

Chairman LIEBERMAN. Thanks, Ms. Rossides. I appreciate your testimony.

Finally on this panel, David Aguilar. Again, we have an Acting Deputy Commissioner. The nominee for Commissioner awaits action in the Finance Committee of the Senate. We hope to have him soon. We are pressing for it to happen. But in the meantime, thank you for your excellent service. As you said, I usually see you in uniform.

Mr. AGUILAR. Yes.

Chairman LIEBERMAN. It is a pleasure to see you either way and we welcome your testimony now.

TESTIMONY OF DAVID V. AGUILAR,[1] ACTING DEPUTY COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. AGUILAR. Thank you, sir, and good morning. Chairman Lieberman, Ranking Member Collins, and Senator Burris, thank you for the opportunity to appear here today as a part of this team to discuss the steps that U.S. Customs and Border Protection (CBP) has taken in response to the attempted terrorist attack on Northwest Flight 253.

The attempted attack on December 25, 2009, was a powerful reminder to all of us that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. Today, I would like to take a little bit of time to describe the role that CBP currently performs in aviation and national security and the enhanced security measures implemented in the aftermath of the attempted Christmas Day bomber attack.

As part of our efforts to screen passengers bound for the United States, CBP is a consumer of the U.S. Government's Consolidated Terrorist Watchlist, which we use to help keep potential terrorists off flights bound for the United States and to identify travelers that require additional screening. Travelers bound to the United States are required to either have a visa issued by the Department of State, or if traveling under the Visa Waiver Program, an electronic travel authorization issued through the Electronic System for Travel Authorization (ESTA) system. ESTA is a web-based system to which individuals must apply for travel authorization prior to traveling to the United States. It enables CBP to conduct enhanced screening of Visa Waiver Program Country applicants in advance of travel to the United States in order to assess whether they could pose a risk to our country.

When a traveler purchases a ticket for travel to the United States, a Passenger Name Record (PNR) may be generated in the airline's reservation system. PNR data contains various elements, including itinerary, co-travelers, changes to the reservation, and may include payment information and type of payment information. CBP receives PNR data from the airlines at various intervals beginning 72 hours prior to departure and concluding at the scheduled departure time. CBP officers utilize what we call the Automated Targeting System for Passengers to evaluate the PNR data against targeting rules. It is important to note that PNR data received by airlines differs and may be incomplete and is inconsistent.

On the day of departure, when an individual checks in for their intended flight, the basic biographic information from the individual's passport is collected by the air carrier and submitted to CBP's Advanced Passenger Information System (APIS). APIS data is far more complete than PNR data. DHS then screens APIS information on international flights to or from the United States against the TSDB, the watchlist, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations.

[1] The prepared statement of Mr. Aguilar appears in the Appendix on page 328.

At nine airports in seven countries, CBP officers are stationed under the Immigration Advisory Program (IAP) that Senator Collins mentioned. Working with CBP's National Targeting Center, IAP officers are provided information on certain passengers who may constitute security risks to our country. These officers can then make no-board recommendations to carriers and host governments, but they do not have the authority to arrest, detain, or prevent passengers from boarding the planes themselves.

While flights are en route to the United States, CBP continues to evaluate the APIS and PNR data submitted by the airlines. At this point, a further assessment on individuals' admissibility into the United States is conducted and a determination is made as to whether an individual requires additional screening prior to admission.

Upon arrival in the United States, travelers present themselves to a CBP officer for inspection. Based on the information garnered during the in-flight analysis as well as the onsite CBP officer's observations, a determination is made as to whether the traveler should be referred for a secondary inspection or admitted to the United States.

Since Christmas Day, CBP has undertaken a number of steps to enhance our current processes. CBP has expanded the information referred to our IAP officers to include any State Department records that contain any national security exclusion realms, something that was not done in the case of December 25.

Chairman LIEBERMAN. Give us an explanation of that in plain language. In other words, what did not happen with Abdulmutallab which would happen now under the change?

Mr. AGUILAR. What did not happen back then, Senator, was that the information provided by the visa office that had information related to what the father had provided——

Chairman LIEBERMAN. The father said, right.

Mr. AGUILAR [continuing]. Was not provided to our IAP officers. That kind of information, which is basically called a quasi-refusal, is now passed on to our IAP officers as a matter of everyday business.

Chairman LIEBERMAN. Right away.

Mr. AGUILAR. Yes, sir.

Chairman LIEBERMAN. What happened to it with Abdulmutallab? It went to the State Department?

Mr. AGUILAR. The State Department provided it by way of their CLASS system——

Chairman LIEBERMAN. Right.

Mr. AGUILAR [continuing]. Into our TECS system, but it never got to our IAP officer because he was not on the watchlist and——

Chairman LIEBERMAN. Tell us what IAP is.

Mr. AGUILAR. I am sorry, sir. That is the Immigration Advisory Program officer that was stationed in Amsterdam——

Chairman LIEBERMAN. So that is a foreign-based American——

Mr. AGUILAR. Yes, sir.

Chairman LIEBERMAN [continuing]. Federal Government employee.

Mr. AGUILAR. A CBP officer stationed in Amsterdam.

Chairman LIEBERMAN. Right. So now, that information would go immediately to that person——

Mr. AGUILAR. Yes.

Chairman LIEBERMAN [continuing]. From the embassy?

Mr. AGUILAR. It goes from the embassy to our TECS system into what we refer to, our National Targeting Center, for aggregation, if you will, with all the other information that we have——

Chairman LIEBERMAN. Right.

Mr. AGUILAR [continuing]. And then that information in total is passed on to our officer stationed foreign.

Chairman LIEBERMAN. Is there a filter applied—I am going to give you a little extra time. I apologize. Is there a filter applied at that point, in other words, standards as to whether it should be included? In this case, we all agree, I think, looking back, his father came in, a respected man. It should have gone right on the watchlist. But, I mean, it is possible somebody could have come in who said they did not know him very well, thought he was acting suspicious. What would happen?

Mr. AGUILAR. Given the same situation, any kind of derogatory information related to terrorism——

Chairman LIEBERMAN. Right.

Mr. AGUILAR [continuing]. That is captured by the Department of State abroad and now put into our system. That is a quasi-refusal that is now captured and provided to our officers. Yes, sir.

Chairman LIEBERMAN. Good. Go ahead and finish your statement. I will give you extra time.

Mr. AGUILAR. On January 10, 2010, we also began additional pre-screening of passengers traveling from non-Immigration Advisory Program locations. Officers assigned to our Regional Carrier Liaison Groups working with our National Targeting Center now make recommendations to foreign carriers to deny boarding to individuals traveling to the United States who have been identified as being national security-related threats that are ineligible for inadmission or who are traveling on fraudulent or fraudulently-obtained documents.

CBP has enhanced reviews of all incoming passenger manifests based on current threats and has increased pre- and post-primary operations. Through intelligence sharing agreements, CBP continues to work with our counterparts in the United Kingdom, Canada, and Mexico, as well as CBP attaches and representatives around the world, to share information as necessary and appropriate.

While we addressed the circumstances behind the specific incident, we must also recognize the evolving threats posed by terrorists and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities.

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, thank you for the opportunity and we look forward to any questions that you might have.

Chairman LIEBERMAN. Thanks, Mr. Aguilar.

We will start with 7-minute rounds of questions.

I appreciate the testimony and particularly the things that have been changed since December 25, 2009. One of the things that is in the process of review, and I will ask you in a moment what the deadlines are, is this question that Mr. Healy referred to directly and Mr. Travers referred to which is how do people get on the Terrorism Watch List and then how are the lists used?

Let me say that as I heard you describing the kinds of information, Mr. Travers, that we might have about somebody being a terrorist or associated with terrorist activities, part of my reaction—you are right. The first two or three you mentioned were pretty clear-cut cases. When you got to the grayer areas, I would say that they were grayer if the question was whether you were going to arrest somebody or capture them in a war on terrorism context. But for me, they were not grayer if the question is whether they raise enough suspicion to be put on a Terrorism Watch List and subject that person to a secondary review, including a secondary screening of his or her body before letting them enter a plane.

Do you understand what I am saying? I invite a reaction to you on that.

Mr. TRAVERS. Yes, sir, certainly, and that is part of the issue that I am sure Director Healy will talk about with respect to our evaluation of standards. The question for us, I think, eventually comes down to one of balance. If we provide every individual and alternative spelling and alternative name variant, and if they are pushed to the airlines for eventual secondary, given the way the mathematics works out, you are starting to look at the potential for millions and millions of names. At what level does that become too difficult for the airlines to handle? I think that is one of the issues that we are struggling with in the interagency group that is looking at this particular problem.

Chairman LIEBERMAN. Yes. My own point of view is this. I understand this can be inconvenient, at some point even burdensome for the airlines, but after all, we are looking at questions of national security here, of homeland security. I mean, at some level, frankly, I say, too bad that the airline has to do that extra work to stop somebody from getting on a plane who might blow up the plane and kill everybody on it and a lot of people on the ground, as would have been the case if the bomb went off on the Detroit-bound plane on December 25.

So it is not that there is not a concern, but I think, ultimately, in just the terms that Mr. Healy mentioned, the classic balance that we need are the weighing of security on the one hand and liberty or privacy, or in some sense convenience or business operations, on the other. It seems to me in these cases, that the great weight has to be given to security.

Mr. TRAVERS. Yes, sir, and I would just make one last point. Certainly, I believe the entire Federal Government is leaning very far forward on putting people on lists, and that has been a bit of a sea change since December 25. I have been doing this now for several years and I will say I am 100 percent certain I never had anybody tell me that the list was too small before Christmas.

Chairman LIEBERMAN. Yes.

Mr. TRAVERS. It is getting bigger and it will get much bigger.

Chairman LIEBERMAN. Well, I appreciate that and I think that is the right way for it to go.

Mr. Healy, one of the things that struck me after December 25, and unfortunately, we all learn from that, is that there were these four levels of lists. TIDE was the largest, and if you were on the TIDE list, it did not subject you to any secondary screening or closer look if you try to get on a plane, which we are focusing on that for a moment. If you were on the TSDB, the Terrorist Screening Database, it seems apparently you were not—they are either subjected to screening, but if you got onto the Selectee List, it required a higher level of evidence, and then the No Fly List, of course, you just were not allowed to get on the plane automatically if you were one of those people.

Picking up in a way from the exchange I just had with Mr. Travers, to me it seems, based on the weighing of the consequences of letting a terrorist on a plane as opposed to the inconvenience of stopping them, if only for a secondary screening—I wonder why we are not consolidating those lists. I mean, obviously, if there is so much evidence that somebody is on a No Fly List, then that is a separate question and that ought to be a separate list. But to my way of thinking, the next list ought to be a real broad one, including the TSDB, which is that there is any evidence of a connection with terrorism, we ought to at least protect everybody else by subjecting that person to a secondary screening. Do you agree or disagree?

Mr. HEALY. I would agree and respectfully disagree at the same time——

Chairman LIEBERMAN. Go ahead.

Mr. HEALY [continuing]. And let me explain. I was under the same position when I first got to the Terrorist Screening Center several years ago as a deputy. The challenge, Senator, is with the list and how we screen it. Right now, the limitation that we have is that the airline is screening. As Ms. Rossides talked about, Secure Flight is going to come onboard, and I think that is a discussion that we need to have between TSA, DHS, and the Terrorist Screening Center, about the advantages that you have with Secure Flight.

Unfortunately, the limitation that we have with Secure Flight, with the Selectee List, and the No Fly List is we rely upon the airlines to do the screening. As we all talk about, it is a balance between civil liberties and protection of the American people. The problem is that when we share that list, we share it not only with the domestic carriers, but we also share it with the foreign carriers.

Chairman LIEBERMAN. Right.

Mr. HEALY. If you share the entire list with the foreign carriers, you have the problem of the security of the list and individuals knowing that they are watchlisted. That is a tremendous security problem. So, again, it is the balancing act right now. Prior to Secure Flight, and again, I think we need the dialogue then, when Secure Flight is on board—and I believe that is going to be at the end of this year and we have been working very diligently with TSA on that—but right now, with the limitations that we have on the screening without Secure Flight, we give it to the airlines, and that includes foreign airlines——

Chairman LIEBERMAN. OK.

Mr. HEALY [continuing]. And that includes potentially giving up the list to foreign carriers——

Chairman LIEBERMAN. All right. So what you are saying is you worry that if somebody is on a terrorism watchlist and they get subjected to secondary screening, then they know they are on a terrorism watchlist. Is that what you mean?

Mr. HEALY. No, sir. If they are on the No Fly List and a terrorist tries to get on a plane——

Chairman LIEBERMAN. Yes.

Mr. HEALY [continuing]. And he is not allowed on the plane, he clearly knows he is watchlisted.

Chairman LIEBERMAN. Right. But you were talking about the privacy of the list when they go to foreign carriers. I thought you meant that some of the people that were on the list might learn they are on the list and that would tip them off that they are being watched.

Mr. HEALY. Right now, TSA and the air carriers randomly screen people.

Chairman LIEBERMAN. Right.

Mr. HEALY. The vast majority of people, like 78,000 that have applied for redress, believe they are watchlisted. The vast majority of them, like 99.3 percent, are not. They are randomly screened.

Chairman LIEBERMAN. Right.

Mr. HEALY. Just because you are subject to additional scrutiny does not mean that you are on the watchlist.

Chairman LIEBERMAN. That is an important point. Right. You are not just screened because you are on the watchlist.

Mr. HEALY. That is correct, Senator.

Chairman LIEBERMAN. Actually, that is a good cover for the watchlist.

Mr. HEALY. Right, and the issue is not the screening. The issue is that we are giving the complete list. I do not think it is prudent to give the complete list to the air carriers with the problem that it may be exposed to different countries, to foreign countries. That is the challenge.

Chairman LIEBERMAN. But here is the other challenge, obviously, and I know we share this goal. If you do not give that list to a foreign carrier, then it is possible somebody on that list who is a suspected terrorist will get on the plane.

Mr. HEALY. And that is the balance that you strike. That is why there is a particular criteria for Selectee, a particular criteria for No Fly, and because of the limitations with the list and who we have to share it with, that is the balance.

I could give you an example of an individual who knew he was watchlisted, came into the country, and changed his identity because he knew he was watchlisted.

Chairman LIEBERMAN. Right.

Mr. HEALY. We only found out because we give the list to the National Crime Information Center (NCIC). The individual was arrested. His fingerprints were taken. It went to our Criminal Justice Information Services Division (CJIS), the FBI's fingerprint department, and he was identified as one of the known or suspected terrorists. He knew he was watchlisted, actively changed his identity

because of that. And so that balance is that I would caution the Committee about giving away the entire list. That is going to create hazards and security issues for us, as well.

Chairman LIEBERMAN. Yes. I hear you, but I still feel that the obligation we have to everybody else on the plane is to check anybody we have reason to suspect of being a terrorist because of the immediate threat of action on that plane.

But my time is up. We will come back to that. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Healy, let me pick up where the Chairman left off. I understand that given how many people are listed on the TIDE list and the fact that the quality of information is not necessarily verified on this broadest of terrorist databases, that it is not practical or perhaps even fair to subject everyone who is on the TIDE list to secondary screening. However, there is a subset of the TIDE list that are foreign individuals who hold visas to come to the United States, and it seems to me that it is imminently fair to subject them to additional screening because as the Chairman indicates, traveling to our country is not a right, it is a privilege, and they have the means to do so because they have a visa.

So in the wake of the December 25 attempted bombing, are you taking a look at that subset of the TIDE list for additional scrutiny?

Mr. HEALY. In short, Senator Collins, yes. And in fact, that is part of the deliberation that this interagency group has discussed and is making a recommendation to the Administration about how to deal with now.

Senator COLLINS. I also want to talk further about the standards that Mr. Travers referred to in his testimony. This is difficult, because you do want to treat people fairly and also you do not want to create a system that is so burdensome and so immense that if you are trying to watch everybody, you miss people you should be watching, and I understand that.

On the other hand, when I look at the minimum standards for getting listed on the various watchlists, they trouble me because they clearly exclude Abdulmutallab. You followed the standards. And indeed, the information in the cable from Nigeria from our embassy did not meet the minimum standards. There is an implementing instruction that actually says that those who only associate with known or suspected terrorists but have done nothing to support terrorism are ineligible for the No Fly List or the Selectee List. So it is easy to see why he did not make the list. He was associating with known terrorists, but you could not pinpoint a specific action.

That troubles me, though, that that is the standard. So I would like to ask you, Mr. Healy, and you, Mr. Travers, I know you are looking at that standard, but in your judgment, is that standard too high for listing someone. Does it exclude people who should be on the Selectee List?

Mr. HEALY. Again, Senator Collins, some of the lessons learned because of the Christmas Day event, we take into consideration, some of the things that you have already mentioned, such as giving credibility to a source and allowing the individual that is interviewing that source to be able to identify credibility. We are taking

a look at the single-source reporting and adding things to it like if you have a respected member of the community, a father talking about his son, that is something that we should take into consideration.

And so, yes, ma'am, all of those issues that we identified as points of learning and lessons learned from the event were taken into consideration and coming up with recommendations again to the Administration about not necessarily how to change the standard. The reasonable suspicion standard is reasonably low, and essentially if you have credible information and reportable intelligence that this individual is associated with terrorism, they are going to go on the watchlist. But how we implement it and some of the restrictions that we had specifically about single-source reporting, labels, things like that, we are looking at and making recommendations.

And candidly, we have been working very hard at that. We have been meeting two, sometimes three times a week and we have very short deadlines and I think we are going to have a product within the next couple weeks, if not the end of the month, or the next month.

Senator COLLINS. Mr. Travers, should an individual who is known to associate with known terrorists be on at least the Selectee List for additional screening?

Mr. TRAVERS. I do not know that I have a solid answer for you. I would associate myself with Director Healy's comments, that we are looking to add flexibility into the system so that we can deal with single-source reporting and individuals who might not fall within the black letter description you had there.

We have asked the collectors, what does this mean? What would this mean for you if you were being tasked to provide into the system nominations on individuals who are just described as associating with a terrorist, and we do not have an answer to that.

I have been an analyst in the community now for 30 years. My guess is that is going to be a very large number, and I would come back to the comment you made to open the conversation, which was you do not want to have so many people on this list that you stop looking at important ones because you are looking at those that are really way down in the noise. But in general, we are enhancing the level of flexibility that any individual has to put somebody on the list, and that is a good thing.

Senator COLLINS. One of the issues that really troubles me is a conversation that I had with a member of the intelligence community who said, you do not understand. We get reports all the time from disgruntled relatives. And I am sure that is true. But in this case, it is a highly respected member of the community whom Nigerian officials have vouched for and referred to our embassy officials, and that is very different and we have to be able to weigh credibility.

I want to quickly, Mr. Travers, ask you one more question in this round. You mentioned in your testimony, and I have heard this before, that thousands of analysts, everyone in the intelligence community who is an analyst, had access to those two critical data pieces about Abdulmutallab. But there is a big difference between

everybody having access to this huge database versus the individuals who are tasked with connecting the dots.

So I would like to get a better sense so I can understand this. I do not think it is a good answer to say, well, thousands of people could have found this information, because that is not the job of thousands of people. Whose job—I do not mean specific names—was it to connect those data pieces?

Mr. TRAVERS. It is a very complicated question, so you are going to have to indulge me for a second. My only point during my opening statement was that I do think this highlights that information sharing, while very important, is not sufficient. The information was shared and people did not connect the dots.

Now, clearly, the function of NCTC and the Terrorist Identities Group and my people in particular who support the watchlisting function, in a perfect world, when we set up the TIDE list and the Homeland Security Presidential Directive (HSPD–6) implementation back several years ago, I envisioned that we would build dossiers on people and that if Russ Travers was an international terrorist, that my people would go out and they would go through all the databases and they will continually update that database and ensure that Russ Travers's record was as complete as it possibly could be.

Three years ago now, we came to the conclusion that because of the growth in the data coming into NCTC, indeed, the community, because the collectors were surging, we were getting these thousands and thousands of reports a day, that we were not even close to being resourced adequately to be able to research Russ Travers in depth, and that is the Umar Farouk problem, the personal name that existed out in the ether that did not get linked with the Abuja cable.

So we made a decision. It was a risk decision, and as a result, we focused far more on populating information into TIDE that was being pushed to us, quality controlling it and not being able to do in-depth analysis. What that meant in practice was that the young analyst that received the Abuja cable with the nomination on November 20 did her dutiful search. She searched Umar Farouk Abdulmutallab and got exactly zero hits because that name did not exist anyplace else in the intelligence community traffic. So, what do we do?

Two responses at NCTC. Conceptually, what we are trying to do is lower the bar. So again, you have this sea of dots. A lot of them are not exploited. We believe NCTC's role is to do that. How do you deal with those 10,000 names that are out there, those 10,000 cables? And NCTC has taken two approaches, one within my group and one within our analytic element.

Within my group, what we are doing is building, per the President's direction, an effort that will do directed sort of enhancement of records, so that we are building the proposal that will have analysts that will do nothing but that. When Umar Farouk's name comes in, whether or not the standard changes in any dramatic way, you have somebody who is below the noise level. They will be focused on going out and searching across all of the databases to see if we as a government know something more about Umar Fa-

rouk Abdulmutallab that can get him pushed to Director Healy's watchlists.

The other function that we are doing with respect to "dot connecting" is building something called pursuit teams, and those exist within our analytic element, currently about 40 people drawn from the community as well as NCTC, and they have kind of a quasi-targeting function in that they are not producers of intelligence, is what NCTC generally does, but instead, they are taking straws in the wind. This is something that is kind of interesting, Nigerians going to Yemen, or an interesting phone number, or something.

And they are digging down into that noise level, that sea of data, and they are following through on that to completion. Completion may be they nominate him for a watchlist. Completion may be that the Bureau opens a case on them or something. This is an experiment, but it is born of the belief that there is so much information out there that somehow we need people that are going to go down and focus in on that information that is below that which is readily identifiable as terrorism.

So those are the approaches that we are taking.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

As I mentioned earlier, and thank you once again for allowing me to make a brief statement, this is something I think about every day, and especially since we had that issue around Christmas-time. I have often wondered, is it a resourcing problem? Is it a tools and resources problem? Do you need more of both to expand the type of coverage we need to help? Is there something that we are missing that we can provide to the various agencies in terms of tools and resources? Let us start with that question, if we could, to anyone who feels it is appropriate to answer. I am looking at all the agencies.

Mr. TRAVERS. I think it is a whole series of issues. As I mentioned to Senator Collins, there is partly a resource issue. If you want to start exploiting more and more of that noise level, the information that just is way below the surface, then there is a resource issue to it.

There is a limitation of the names-based system, so all of us are moving towards biometrics as quickly as we can because that is part of the answer.

There are some technical issues, for sure. Those technical issues merge with policy and privacy issues in a hurry, in that I mentioned the 30 networks that we have coming into NCTC. You can not just commingle that data. Why? Because you have tremendous amounts of U.S. persons data in some of those networks. And so this gets into a very difficult area for us in terms of the bleeding over of foreign and domestic, and those are some of the issues that Mike Leiter is looking particularly hard at.

And that gets to the issue of kind of Google-like searches. As I mentioned, we can do Google-like searches across some of the foreign networks, but you can not do a search that goes out against the FBI stuff or a search that goes out against the CIA material and pull things back. And so those technical limitations are born of privacy, policy, and security issues.

Mr. HEALY. If I may add, the challenge is also, as Mr. Travers pointed out, trying to identify these terrorists. There is no Driver's License Bureau where bin Laden goes to and says, "I need my terrorist card." These individuals are identified by fragments of information. They are identified by overheard conversations. They are identified by a source saying, this guy is involved in it. So it is not a black-and-white system. It is a system that we continue to search and try to identify these nuggets of information so these individuals are watchlisted. It is a balancing act between civil liberties and the protection of the American people.

So it is a challenge, and because of the name-based system, it is always going to be a challenge. In some cases, on the No Fly List, you need name and date of birth. The reason for that is because that is how we identify people. So it is a challenge just with the whole process and trying to identify these individuals.

Every day, I talk to my staff and tell them, if you make one mistake, people could die, and all we have to do is make one mistake. We have to be right every single time, and all the terrorist has to do is be right one time. So it is always going to be a challenge. Resources are always a challenge——

Senator BROWN. I guess what I am trying to ask is, obviously, we are dealing in budgetary issues coming up. The safety and security of anyone traveling in the United States is one of my top priorities. It would be helpful to me to know in real numbers and in real needs, what do you need to do your job? Are we missing something? Do we need to do more in one area or less in another? Do we need to shift? I mean, fact versus fiction. What do you need to do the job the best you possibly can?

That is one of my main concerns. So if there is anything, maybe offline I can meet with somebody to let me know what that is, because we are formulating those priorities and I want to make sure that we can keep people who are traveling in our country safe. So thank you for those answers.

I just had one other question. If there is somebody who is actually on the various lists and they are—in fact, I get a lot of these calls, even when I was a State Senator. How do they get off of it? If they clearly do not have any terrorist ties, it is just by some similarities of names. Is there a process or somewhere where you can direct me where I can direct these people to get off that list?

Mr. HEALY. There actually is, and we work with DHS. Did you want to go over that?

Ms. ROSSIDES. Yes, sir. DHS has a redress process where persons who think that they are on either the No Fly or Selectee List can apply. It is an online process. And we work with the TSC to make sure that the individual is actually cleared. They then get a letter saying that they are cleared. They get a redress number so that when they book travel in the future, they can actually reference that redress number, and it should automatically clear them so they do not have a continuing problem.

Senator BROWN. Where do I direct them?

Ms. ROSSIDES. You could direct them to the TSA Web site where there is a link there for the application to apply for redress.

Senator BROWN. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Brown

I appreciate Senator Brown's question. These questions do come up and it does seem to me, though there clearly is a problem of false positives, such as the case with an Arab name where there are a lot of similar names in the phone book, or the cases we have heard about here where Grandma gets stopped because she has a similar name, or the young boy who was stopped a few times, but that can not be an excuse for limiting the names on the watchlist because there is some reason to put somebody else with that same name on the watchlist and they belong there.

And so I think the redress process you have set up is a good one. I do not know what latitude you can give your TSA people at the site, CBP at the site, or airlines at the site of entry. I guess anytime you have any latitude, it is a problem. But it just seems to me if you have a 7, 8, or 9-year-old boy and he has the same name as somebody on the list, it is pretty obvious that he is not the one and he ought not to be stopped from getting on the plane.

Ms. ROSSIDES. Exactly, Senator. In fact, what will happen is—particularly when a child shows up at the ticket counter—there is an actual call made between the carrier and TSA to immediately rectify that problem.

Chairman LIEBERMAN. That is very good.

Ms. ROSSIDES. We try to do it in real time, as well, so that we can clear up those kind of situations.

Chairman LIEBERMAN. So that case would not happen again.

Ms. ROSSIDES. It does not happen that frequently, sir.

Chairman LIEBERMAN. Yes. So it has become an urban myth. It keeps being cited. Thank you.

Senator Carper, we have welcomed in absentia for the moment Senator Kaufman and commented on the disproportionate representation that the State of Delaware now has on this Committee.

Senator CARPER. Our Congressman wants to be on it, too, probably. [Laughter.]

That is a story for another day.

Chairman LIEBERMAN. All right. Thank you.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. So does our County Executive from Northern Delaware.

But we welcome Senator Kaufman. I just came from a meeting with him and a bunch of folks from our State. I am sure he will get here if he can.

I want to certainly welcome Senator Brown. I am delighted you are with us and we are going to take one of those congressional delegations (CODELs) and go to Afghanistan and Pakistan next month. Sometimes our staffs go on staff delegations (STAFFDELs) and we have had a couple of them who went over from our staff, I think Senator Lieberman's and Senator Voinovich's staffs also, among other places they visited were Yemen and Saudi Arabia and they spent a little bit of time in Holland and in Germany.

I will not get into Saudi Arabia and Yemen, but one of the things that they heard about in Holland, especially with respect to the Amsterdam airport, was the kind of behavior assessment or profiling that takes place at some of those airports. The Israelis are, I think, especially noted for these techniques.

But I am told that you have airport security officials who try to identify and prevent bad guys from getting on airplanes and causing trouble. They do it, in part, by observing the passengers, I think before they get to the gate, maybe after they leave the gate. I understand that the airports position well-trained personnel at various points before and after ticket counters to ask questions politely, to scrutinize facial expressions, to check out body language and speech pattern.

I do not know if this is a good idea or not. The Israelis think it is and some other countries do, as well. But I would just be interested in hearing the thoughts of our witnesses today on this type of screening and to ask if you think there is something that we can learn from what some of these other countries are doing.

Ms. ROSSIDES. Yes, Senator. Actually, TSA has worked with the Israelis and other countries, and we do have a Behavior Detection Program in TSA that we have deployed across U.S. airports. We have several hundred officers that are trained as Behavior Detection Officers, and they actually look for the behavior anomalies that you describe.

Senator CARPER. Could you be more specific? I do not want you to talk out of school, but could you give us some idea of what you are looking for?

Ms. ROSSIDES. Most of it is sensitive security information that I could not give you and——

Senator CARPER. I understand.

Ms. ROSSIDES [continuing]. We would be happy to provide you a briefing in a closed session.

Senator CARPER. OK.

Ms. ROSSIDES. They do look for anomalous behaviors that should not be displayed by the everyday traveler. When they do that, they will respectfully approach the passenger, engage them in some simple conversation. Depending upon what they glean from that discussion, they may actually refer them for secondary screening in the checkpoints. We have several hundred of these across most of the largest airports here in the United States.

I also would say that some of what we are continuing to learn is really sharing best practices from our counterparts like the Israelis. This really is a global effort, and particularly in the aftermath of December 25's event, what we have seen is the willingness of our global partners to actually come to us and the Israelis to learn about our Behavior Detection Program and also to learn about the technology that we are now deploying across U.S. airports. And I am happy to say that since December 25, we have had at least eight, if not closer now to a dozen, countries that are going to be deploying this advanced technology at U.S.-bound gates and terminals.

So there is quite a bit of information sharing and best practices that we are doing.

Senator CARPER. Good. Do any other witnesses want to comment on this, please?

Mr. AGUILAR. I would just add, Senator, that with Customs and Border Protection, both foreign and domestic, at locations where we are foreign deployed, the same type of training is given. It may vary a little bit, but the same type of basic training is given to the

officers in order to detect that anomalous reactions, if you will, to being confronted by officers.

Senator CARPER. Thank you.

Dr. Stephen Flynn, of the Center for National Policy, who is, I think, fairly well known and a respected homeland security expert, recently met with my staff and with me. He said something that hit home regarding aviation security. He said basically, and I am going to quote him, "In searching for that needle," like a needle in a haystack, "we need to take some hay off the stack and ensure that the screeners be logical in their approach."

And this may follow up on something that Senator Brown was saying, but I asked him to explain what he meant. He is essentially saying that, for example, if you see a great-grandmother and a 6-year-old child, you might want to place a little less scrutiny on them than someone else who is maybe younger or maybe older and someone who might realistically pose more of a threat.

Ms. Rossides, if you would please just comment on what Dr. Flynn said.

Ms. ROSSIDES. Yes.

Senator CARPER. And let us know if the screeners are trained to adapt their techniques based on the age of the passenger.

Ms. ROSSIDES. Well, sir, the challenge that we have is balancing the requirement to screen all passengers and to actually focus our officers' attention on the right passengers per se as you describe.

I will tell you, based on the intelligence that I see every day, that I would not sit here and say that there would never be an elderly person that could be used to be a carrier of a bomb on an airplane. I have seen around the world people used for this purpose who are in wheelchairs. I have seen them use young people. And that is our challenge.

But what we have designed here in the United States and what our global partners are doing with us is a multi-layered approach so that we really do, through our Behavior Detection Program, through our use of advanced technologies, through what we are doing randomly with Explosives Trace Detection Technology, look at passengers maybe a second time or give some random unpredictability to the system. We are not always predictable, and you can not always guarantee that somebody of an age type or certain characteristic will or will not be screened.

But it is a challenge, and we will modify what we do, and sometimes TSA does get criticized, as to why are we focusing on toys or something. I will tell you, what we do is based on the intelligence that we are getting.

Senator CARPER. Would it be appropriate to share with us and the broader public, just some examples of things that you have found? Were there toys and things that are in wheelchairs? But is there something you can share with us? I heard on National Public Radio (NPR), I do not know if it was NPR, but I was driving to the train station last week and they were reporting outrage. A young child, maybe a 2-year-old child, maybe handicapped, the father was a policeman and was scrutinized. Can you give us some examples of why it is actually important that we do that scrutiny?

Ms. ROSSIDES. Yes, sir. Every day, I will tell you that we see things coming through checkpoints in the United States that are

amazing, that people are trying to secrete on their persons, in wheelchairs, and in canes. People will conceal long knives or swords in canes. At least a couple of times a year, particularly around the holidays, we find guns in teddy bears. We find component parts in children's toys. It is amazing what we see. We actually do put out on our Web site information that will identify things that we are looking for and why, explaining at least why we have to take a closer look at some of these things. The officers get information on a daily basis in their shift briefings about those kinds of very common items that we are actually seeing people conceal things in, trying to get on board the aircraft.

One of the things that we see as our responsibility, particularly this year as we are rolling out this advanced imaging technology, is our very significant responsibility to educate the traveling public about the benefits of this technology, about their options to go through this technology or not, and really to understand why this is an increased detection capability for us that will actually ensure their greater safety.

We do try to inform the public when we can on things that we are seeing and why things are subject to the screening as they are.

Senator CARPER. All right. That was very helpful. Thank you very much.

Thanks, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Carper.

That was helpful. I will bet the traveling public will be encouraged to hear about the behavior identification work that is being done without apparent knowledge. It is important.

The other thing I do want to say, and Mr. Travers referred to this briefly in another regard, that the more we move to a biometric system of identification, obviously, the problem of false positives is reduced or eliminated totally, and that is another reason to try to do that as quickly as we can.

Mr. Healy, I want to clarify. Did I hear you say that you thought the process of review of the standards for inclusion in the use—terrorism watchlists and the use of the watchlists that is being carried out pursuant to President Obama's directive post-Christmas Day bomber, that you thought it would result in recommendations by the end of this month, or were you referring to something else then?

Mr. HEALY. No, sir. I do not want to cut the group off—but we have been working very hard and I think we are wrapping it up right now. We have some very tight deadlines, much tighter than I would have expected, but the team is working very diligently and I expect to have some recommendations very soon.

Chairman LIEBERMAN. So this is an interagency process. Are you chairing that as the head of the TSC?

Mr. HEALY. Yes. I would say it is a joint between myself, Mr. Travers, and the White House, going through the issues that were raised and specific issues of the threat issues that we have.

Chairman LIEBERMAN. Right.

Mr. HEALY. We have representatives from everyone here that participates in that, as well.

Chairman LIEBERMAN. So will you make a recommendation to Homeland Security Advisor John Brennan or the President, or will you actually adopt a change yourself?

Mr. HEALY. We are actually making a series of recommendations to the Deputies' Committee that Mr. Brennan chairs——

Chairman LIEBERMAN. Right.

Mr. HEALY [continuing]. That will be obviously forwarded up to the White House. We have had a couple of sessions with the Deputies' meetings, just basically giving them an indication of where we are at, some interim issues that we have identified, and gotten some very specific guidance about how to proceed. So that process is ongoing and continue to mature.

Chairman LIEBERMAN. Well, we look forward to the results of that. I appreciate your work on it.

But Mr. Travers, I just want to clarify something in that regard. Director Leiter, when he was before the Committee last time, I am pretty sure said that the No Fly List, that is the top category, was expanded in the aftermath of the Christmas Day bombing attempt. Can you describe for us, generally speaking, what has changed?

Mr. TRAVERS. I will actually defer to Director Healy. There have, indeed, been significant numbers of people added to the No Fly List, and since Mike Leiter was here, far more.

Chairman LIEBERMAN. Yes. OK. Mr. Healy.

Mr. HEALY. Right. Just so we are clear, the criteria for No Fly-Selectee has not changed.

Chairman LIEBERMAN. Right.

Mr. HEALY. What has happened that I think Mr. Leiter was referring to is based on the intelligence as a result of that, we were directed to move a number of people on Selectee and No Fly, very similar, Senator Collins, to what your concerns were. As a result of that——

Chairman LIEBERMAN. In other words, to move them from Selectee to No Fly, or from——

Mr. HEALY. Move them from TIDE into TSDB, TSDB into Selectee, Selectee into No Fly——

Chairman LIEBERMAN. So it was all up the chain of the list.

Mr. HEALY. And it was not just ticks. It was, if you identify this particular——

Chairman LIEBERMAN. What is a tick?

Mr. HEALY. Stages. You did not go into the TSDB and then move to Selectee. Based on the threat reporting, individuals were moved onto No Fly. Based on the reporting, individuals were moved into Selectee. Based on the reporting, individuals were moved from TIDE——

Chairman LIEBERMAN. So there was new reporting, or was it that you went back and took a second look without changing the standards?

Mr. HEALY. It was a culmination of the threat that we had and the intelligence, and as a result of that, we were directed by the White House to move a number of people, and the process right now in that movement is a deeper dive on all those individuals that the agency and the FBI are participating on to determine if there is any additional information, and that process is ongoing.

Chairman LIEBERMAN. Right. But the other process that you are working on that we talked about a moment ago, that you will report to Mr. Brennan and the Deputies' Committee at the White House, is standards for inclusion on the various lists——

Mr. HEALY. Yes, sir.

Chairman LIEBERMAN [continuing]. And the way in which those lists are used.

Mr. HEALY. Yes, and to address issues that Senator Collins pointed out, that if you have a single source reporting——

Chairman LIEBERMAN. Right.

Mr. HEALY [continuing]. Should you allow that individual that is talking to that potential source to be able to judge his credibility.

Chairman LIEBERMAN. OK.

Mr. HEALY. Issues like that have been raised up and are being forwarded.

Chairman LIEBERMAN. Let me ask, I guess primarily Mr. Healy or Mr. Travers, for some clarity on these technological questions, because I was surprised in your opening statement. I do not think it was an absolute statement, Mr. Travers, when you kind of indicated that the Google-like searches that Senator Collins and I referred to cannot be done by the National Counterterrorism Center. In other words, we are accustomed to this remarkable ability to search an enormous number of databases quickly and have the information come up through a search process like Google.

My impression from Mr. Leiter when he testified here is that now, your analysts at the National Counterterrorism Center cannot—and let us simplify this. Let us just take the name Umar Farouk Abdulmutallab. They can not search that across all the databases like that. They have to sort of dig down into each database. Am I correct?

Mr. TRAVERS. Yes, sir. As I mentioned, there are 30 or so networks that come into NCTC. We clearly cannot do a Google-like search across all 30 of those networks for some of the policy-privacy reasons I suggested. My analysts within the Terrorist Identities Group can do a Google-like search that will take them out to the terrorist message traffic that will come in from many of the organizations that will go into a data repository. They can search across that. And with TIDE, actually what they find is the same problem you have if you do a Google search at home. You may get so many reports back——

Chairman LIEBERMAN. Yes.

Mr. TRAVERS [continuing]. That you get thousands, and that does not help you very much, either. There is no question that an analyst could have after-the-fact fashioned a query that would have been very precise and you would have gotten the limited reporting that exists on Umar Farouk. The challenge is knowing what you are searching for.

Chairman LIEBERMAN. I understand all those problems and I accept their reality, but when you answered the question just now, you referred again to the privacy concerns about searching all the databases at once. But do we have the technological capability at the National Counterterrorism Center to quickly search all the 30 networks of information you have coming in?

Mr. TRAVERS. The technological capabilities flow from the policy enablers and there are some unanswered questions on both the operational side as well as the privacy side that limit our ability to implement a technological solution. I think if our chief information officer (CIO) was here, she would tell you that the technical issues are not the long pole in the tent.

Chairman LIEBERMAN. Well, that is sort of both encouraging and discouraging, I must say, because I do not want to diminish privacy concerns, but to me, they must be secondary to the quest—just as you said, one mistake and people get killed. One time a terrorist breaks through the networks and that is all they have to do, one time and they are successful.

The reason it is encouraging, I thought it was that we did not have the right equipment, the right information technology, but in a way you are saying to me now, if I hear you correctly, that it is really more a question of the standards that we have that stop your analysts from searching all the networks at once.

Mr. TRAVERS. Yes. Our CIO Office for a number of years now has been looking forward to how do you build a data layer that will allow you to do searches that will get you to all of the data.

Chairman LIEBERMAN. Yes.

Mr. TRAVERS. I mean, if you carry this to its logical extreme, people begin to think you are talking about Total Information Awareness (TIA), and Admiral Poindexter and so forth. Well, clearly, that is not the direction you want to go. However, you do want to get to the point where you can search across all data that might have a terrorism nexus. Some of that data may be DHS data. It may have asylum seekers, refugees, and U.S. persons in it. Where is the right balance? And those are some unanswered questions.

Chairman LIEBERMAN. My time is up. I must say, and I think the whole Admiral Poindexter brouhaha ended up sending some wrong messages, because I thought—it may have been because of his personal background, too—he was asking reasonable questions. They may not have been perfect questions, but he was trying to push the technology to make it maximally helpful to us in our quest to stop people from——

Mr. TRAVERS. Yes, sir.

Chairman LIEBERMAN [continuing]. Doing us damage.

Mr. TRAVERS. We would agree that there is no question that a human being is not going to be able to go through all that data.

Chairman LIEBERMAN. Yes, exactly.

Mr. TRAVERS. You have to use technology.

Chairman LIEBERMAN. Yes. Thank you. Senator Collins.

Senator COLLINS. Mr. Chairman, I am going to yield to Senator Brown first because he has a scheduling conflict.

Senator BROWN. Thank you, Senator, and Mr. Chairman, I appreciate it.

I just had one quick question, probably to Mr. Healy. When you are making that recommendation to the President, I am not sure if this is the appropriate vehicle to do just that, but do you recommend how the people who are actually caught trying to hurt us, such as the Christmas Day bomber, should be treated in terms of prosecution or interrogation? Will there be that type of recommendation within what you are doing?

Mr. HEALY. No, sir. I was specifically asked to take a look at the watchlisting standards and No Fly, the Selectee, how that particular process worked, and that is where I am focusing it. With regard to what you just asked, no, that is beyond——

Senator BROWN. Who will be responsible for making those recommendations to the Administration?

Mr. HEALY. I am not sure, sir. I would defer that question and I would like to get back to you, if I could.

Senator BROWN. If you could, that would be great.

Senator I appreciate you deferring, and thank you, Mr. Chairman.

Senator COLLINS. Thank you.

Ms. Rossides, I think you preformed a very important service today by reminding us that we cannot have profiles in our mind of what a terrorist looks like and that a terrorist can use a young child or an elderly person in a wheelchair. We should all be reminded of that by the story that broke in the news today, where a blonde, green-eyed woman from Pennsylvania turns out to be suspected of terrorist acts. So I think that is a very good reminder to all of us.

I recently was returning from Zurich and had to go through a full pat-down and I thought, what a waste. I have shown my ID. It is clear who I am. Why am I having to go through this? But the fact is, that random quality of selecting people is important, and I think you have given us a good reminder of that today.

I want to give you a chance today to respond to concerns that have been raised by various outside groups—I think one is the Electronic Privacy Information Center—about the full-body scans. I would like you to address not just the privacy concerns that have been raised, but also the health concerns. I happen to know that TSA looked at the health concerns and did an analysis of the exposure to the radio waves, but I do not think the public at large knows that. So if you could comment on both of those issues.

Ms. ROSSIDES. Yes, Senator. First, with respect to the privacy, from the very beginning when we started to test this new technology, we filed a Privacy Impact Assessment, and we held a lot of meetings with privacy groups and various interest groups in our wide net of stakeholders. We have gone to the point where, today, where we have this technology deployed, there is a clear separation between the Transportation Security Officer (TSO) or the officer who is facilitating the passenger going through that technology and the actual officer who is seeing the actual image of that passenger. The two officers never overstep so that the officer that is with the passenger never sees the image of the passenger in the technology and the officer that is viewing that image is located in a remote viewing room.

The standards for the officers who are viewing those images is very high. They are not permitted to bring cellphones into the viewing area. They are not permitted to take a picture. And most importantly, the technology is set up such that the operator cannot store that image, they cannot copy it, they cannot transmit it electronically to another work station. So we have taken a lot of measures from a privacy standpoint to protect the traveling public.

In addition, the passengers are advised that it is optional. If they do not want to go through this technology, they can have alternative means of screening.

The health and safety aspects of it were also very important to us from two standpoints—first, from the traveling public's standpoint for every passenger, as well as for our officers who would be near that equipment all day long. We had a number of Federal agencies, including the Food and Drug Administration, and the National Institute of Standards and Technology (NIST), look at the standards that the manufacturer certifies to in terms of health and safety. We also asked Johns Hopkins University's Applied Physics Lab to take an independent look at the technology and give us their independent assessment of its safety.

And in essence, for the two different types of technology, the exposure is equivalent to less than 2 minutes of air time in an airplane at full altitude or less than 10,000 times your radiation or your exposure when you are on your cell phone. So it is very minimal. You would have to fly, I believe the standard is, 15,000 times a year to be exposed to anything that would reach the very baseline of a question in terms of the health and safety standards.

Senator COLLINS. Thank you. That is very helpful testimony for us to have.

Mr. Aguilar, I want to first tell you and thank you for the extraordinary service we have had from a detailee, Matt Hanna, from your agency. He has really added to our knowledge of CBP and we appreciate it.

I want to talk to you about the screening computer program that is known as the Automated Targeting System. This is intended to identify travelers for additional screening even if they are not on the terrorist watchlist. So again, it is part of this layered approach to security.

Now, following the Christmas Day attempted attack, DHS started requiring passengers who are citizens of or traveling from one of 14 countries to undergo additional physical screening before boarding a flight to the United States. What worries me about that approach is it seems to me to not really be risk-based and to encourage terrorists to travel through other countries or use citizens of countries that are not on the 14-country list.

I can understand why we would want to put Yemen, for example, on that list, and that may make sense. But it seems to me that we know that terrorists are smart. They are adapting constantly. And when we advertise that these 14 countries are going to be subjected to additional screening, we just encourage them to go around that.

Why instead would not we make increased use of the Automated Targeting System to identify high-risk travelers rather than doing this blanket approach?

Mr. AGUILAR. Senator, you hit on something that is absolutely critical to helping secure this Nation, and that is what you are referring to is addressing the unknowns. When we talk about the watchlisting, when we talk about the biometrics, when we talk about the knowns, that is, frankly, in our world, the easy part of finding the bad people. What you are referring to is finding the unknowns.

Taking Umar Farouk Abdulmutallab, for example, had his father not come in with that piece of information, he would have been completely unknown to us. But by utilizing the Automated Targeting System (ATS), the targeting system that we utilize, we take into account tidbits of intelligence that may or may not be in the TSDB. We take what we believe to be known or might be known travel routes coming into the United States, origins, things of that nature.

So that is managing risk. That is what that system is specifically used for in order to address the unknowns that might be coming into our country. We use that on a constant basis. It has been very successful.

Now, as to the 14 countries, and I will leave the rationale for the 14 countries' delineation to my partner from TSA, but after December 25, 2009, we needed to do everything possible to ensure that not only the knowns, the unknowns, but any other gap could have been closed, and that was the original reason for the 14. But again, you hit on something that is absolutely critical that we not forget about, and that is the unknowns trying to get into this country that we have absolutely no idea. We have just tidbits of information that we basically address by focusing our intelligence, by focusing our efforts on what we do know of modes, means, or rationale as to how they try and get into this country.

Senator COLLINS. Thank you. Mr. Chairman, just one closing comment, if I may.

Chairman LIEBERMAN. Go right ahead. I actually have a few more questions——

Senator COLLINS. Oh, you do? OK.

Chairman LIEBERMAN [continuing]. So if you want to do another round, Senator Collins, fine.

Senator COLLINS. That sounds great.

Chairman LIEBERMAN. Good. Thank you.

In the last round of questions, I asked about the ability to do a Google-like search of a similar name or subject across all the networks, but I wanted to ask you also—we talked about this last time with Mr. Leiter and others who were here, and this, I did not understand very well—I know that in the private sector, there are some computer programs that do not search for the exact same name but have the capacity to make connections of words or topics.

In this case, part of the frustration was, as I mentioned in my opening statement, we knew from one intelligence source that there was a Nigerian training with al-Qaeda in the Arabian Peninsula. We had another intercept that suggested something might be happening around the Christmas holidays. We had another intercept that identified a man by only his first two names, Umar Farouk. And then, of course, we had the father come into the embassy.

And then this problem we have now is this enormous amount of data that you said—the numbers are stunning, 10,000, essentially, new names suggested every day, more data collected, primarily by the National Security Agency (NSA), I presume, every day than is in the Library of Congress. So this is impossible for humans to sift through in a timely way.

To your knowledge, are there systems, software, programs that we can or should acquire that can make a stab at not the same name everywhere, but bits of information that a quick search may tie together?

Mr. TRAVERS. Yes, sir, and as I suggested, we are utilizing many tools and are always looking at others. The issue of alternative names is a relatively simple one, I think, that probably all of us at this table have capabilities resident in our departments and agencies that will deal with cultural differences and spellings and so forth, and so we have that one, I think, relatively licked. It does present problems when you are trying to do this on a massive scale and correlate it with other data because now you have 100 different spellings of one name and they reach out and touch other data and now do you have false positives? Absolutely.

Chairman LIEBERMAN. Yes, but what about the case that we had with Abdulmutallab. Is there a computer system that might conceivably have picked out those similarities that I just mentioned—Nigerian, Umar Farouk, then the father comes in and cites Umar Farouk Abdulmutallab?

Mr. TRAVERS. If you tailor a query, absolutely. Then it is a very simple process.

Chairman LIEBERMAN. Give me an example of such a——

Mr. TRAVERS. If you had searched on "Umar Farouk" and "Nigeria" and allow it to use alternative spellings, then it is an easy question. It was, just as Mr. Aguilar indicated, if you know what you are looking for, then the query is easy.

Chairman LIEBERMAN. Yes. So we have the equipment to do that kind of search now across the databases?

Mr. TRAVERS. That is correct. My analyst could have, in fact, found that linkage if she had known to make the query.

Chairman LIEBERMAN. Right.

Mr. TRAVERS. There are things, latent semantic indexing, that will allow you to generate new knowledge, you can pour in many cables, and they don't necessarily find a direct linkage, but because they can learn, if we are smart enough to program the algorithms, that they can connect pieces of information. We are certainly experimenting with that, as well, and certainly there is the next generation of analyst notebook kind of things which make pretty pictures and link a lot of people together.

Chairman LIEBERMAN. Right.

Mr. TRAVERS. Frankly, any analyst will tell you that is just the beginning. Now you have a tremendous amount of information. Now you have to burrow down into one correlation between two individual points.

Chairman LIEBERMAN. Well, technology has taken us very far very rapidly, so hopefully it can help you sift through all that information that comes on your desk every day.

Commissioner Aguilar, let me go back to that question about when you get the information about passengers coming on a plane. A lot of times, including with Abdulmutallab, we actually did not have the information until he was on the plane. I wonder what you think about creating a rule that we thoroughly screen each flight's passenger manifest against all our databases at least 24 hours, if not longer, before the airplane is set to depart, understanding that

not everybody will be on a database 24 hours before, but most of the passengers probably will be.

Mr. AGUILAR. Right. Yes, sir. The more information we have available to us quickly is going to enhance our capabilities to affect the intent of anybody trying to board a plane coming towards us.

Today, we use what is known as a Passenger Name Record, the PNR.

Chairman LIEBERMAN. Right.

Mr. AGUILAR. But as I stated earlier, it does not give us all of the elements that we need. We are working with the civil aviation industry to try and get them to get us the information that will get to us up to 72 hours before so that we can start running the passengers against our systems.

I believe you are aware, also, that prior to actual boarding, 30 minutes before, we do get the full biographical information of the passengers when they either swipe their passport or the carrier provides us the batch information that will give us those capabilities. But to the degree that we can get more information as quickly as possible, it will be a tremendous enhancement to our capabilities to run against all the databases.

Chairman LIEBERMAN. I appreciate that answer. So, really, you are pushing it now to see if you can get that information up to 72 hours before flight departure.

Mr. AGUILAR. Yes, sir. The PNR data, yes. We start at 72 hours, at 24 hours, 8 hours, and one hour before, and then we get the APIS data at 30 minutes before boarding.

Chairman LIEBERMAN. I guess it is a question of whether you can get the APIS data earlier than 30 minutes before, because that is really the more helpful data.

Mr. AGUILAR. That is going to be the data that gives us the full information on the passengers that are going to be on the manifest, yes, sir.

Chairman LIEBERMAN. Please let us know if there is anything we can do legislatively to expedite that process for you. That is really important.

Mr. AGUILAR. Thank you, sir. We are working closely with the industry right now, but we will get to you if that does not work out.

Chairman LIEBERMAN. Good.

Administrator Rossides, I want to ask you a final question. It is my understanding that, and you refer to this somewhat in your opening statement, on Christmas Day last year, shortly after that Northwest Flight 253 landed in Detroit and authorities began to investigate the incident, somebody at NSA determined that a pilot should be alerted to what authorities knew at that time. What I have been told was that TSA alerted all transatlantic flights that someone had tried to light a combustible substance and that pilots should notify passengers that all carry-on items needed to be stowed one hour prior to arrival. The message was sent by TSA via the Federal Aviation Authority (FAA), by the FAA alert system in every cockpit of every plane, and I think two subsequent messages were also sent which contained some additional information.

So I wanted to ask you two questions, both looking back but also looking forward. Obviously a lot of this is quite commendable. Who at TSA made the determination to send those particular alerts?

And then my question looking forward is, if my information is right, why was a decision made to send them to only the transatlantic flights? In other words, given the imperfect information we had at that point about what was going on and the knowledge that we had of sometimes these attacks being sequenced, not just one at a time, why didn't TSA send those alerts to all aircraft flying into, across, or out of the United States?

Ms. ROSSIDES. Yes, Senator. Actually, I made the decision. I was on the call in the aftermath, as we got word of the flight in Detroit. We had FAA on the bridge call with TSA and I made the decision to have FAA notify those pilots.

We did, as the information was very rapidly coming in to us, we did a very quick assessment of how many flights for the next 8 hours were inbound to the United States, and 128 of them were inbound from Europe. It was my decision to notify those, based on the intelligence that we had, based on the fact that this particular flight had come from Europe.

As part of our process after every one of these incidents, we do a hot wash and look at what should we do differently, and we have already added it into our Critical Incident Plan, that if we were to face another incident like that, we would notify additional carriers beyond those that we had in our window in those 8 hours in that specific region. It is one of the lessons learned from that day.

Chairman LIEBERMAN. Very good. So in other words, if that, God forbid, happens again, you would notify carriers flying in the United States as well?

Ms. ROSSIDES. Right.

Chairman LIEBERMAN. Thank you. Thanks for the initial decision you made and thanks for the lessons learned.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Ms. Rossides, you looked as if you wanted to comment when I was having the exchange about the 14 nations that were listed versus greater use of the ATS. Would you like to comment on that issue?

Ms. ROSSIDES. Yes, Senator. It was actually TSA's decision to identify those 14 countries in the immediate aftermath of the Christmas Day event. Most of those 14 countries are listed on the Department of State's Counterterrorism Report. It is the Counterterrorism Report from 2008. It is actually on their Web site, and those are reported and identified as state sponsors of terrorism or safe havens for terrorism. That was part of what we looked to do.

We were looking to do some very immediate things to literally blunt what could have been another attack, and so that was one of many measures that we put in place in literally the days and hours after the Christmas Day event and in the subsequent weeks. It is something that we do all the time, and we are now in the process of reviewing that list with the Secretary as part of the initiatives that she has to look at in building more of a global information sharing capability.

So something that we will continue to look at is those countries. But it was a blunt measure because we just did not know who else was traveling and where they were traveling from.

Senator COLLINS. Thank you.

Ms. ROSSIDES. Thank you.

Senator COLLINS. Mr. Travers, I just want to pose my final question today to you. I was a bit concerned in the discussion you had with the Chairman about the databases across government that you pointed to policy and privacy reasons why there could not be a search across these databases rather than technical reasons. And the reason I am concerned about that is we are trying to get away from the stovepiping. We want that exchange.

Now, I recognize the concern with U.S. persons versus foreigners, but we tried to break down a lot of those walls when we passed the 2004 landmark law. What are some of the specific policy and privacy standards that prevent you from searching across databases?

Mr. TRAVERS. I do not pretend to be a privacy lawyer, but I will tell you that we have been working for many years to get data sets from different departments and agencies. We have had a fair amount of success with getting an analyst native access. That is, they can go in and log onto one of those 30 networks and access another department or agency's data set.

What gets to be far more complicated is if we want to actually ingest a full data set so that we can apply the kinds of tools that we were talking about earlier. That gets harder for departments and agencies because now they are basically giving up control of that data, and generally, it is not either foreign or U.S. persons. Increasingly, we have data sets that are commingling data. They have both there. And so this provides a complicated problem set for the different privacy advocates and lawyers at the different departments and agencies about how far they can or should go with respect to allowing individuals like me, an intelligence community officer, to be pulsing around their data.

And so we have been working with probably 12 or 14 different departments or agencies. We have had some success with some, lesser success with others.

Senator COLLINS. That is an issue, Mr. Chairman, that I think we are going to need to proceed to pursue further.

Chairman LIEBERMAN. No, I agree. It has been a little unsettling to hear some of the answers.

And again, I appreciate everything the four of you have done. Of course, I am very proud of NCTC. I do not minimize the difficulty of these decisions, but I do think, ultimately, in these cases, security has to be given much more weight than privacy because of all that is involved.

My guess is, if you ask the American people what they would want us to do, they would say, I want you to protect my security. I am willing to give up a little of my privacy for that.

We will continue this discussion. But again, this review began on the 5-year anniversary of the 9/11 Commission legislation, which established the Director of National Intelligence (DNI) and the NCTC, and, of course, we have now been longer than that into the experience in the Department of Homeland Security. So we are way more protected. The American people are way more protected than they were on September 11, 2001. That is the good news.

But we can do better, and that is part of our job to continue as the oversight committee to push on this. So the changes that you

have made in various ways across the agencies represented here since Christmas Day are constructive and helpful and increase security, and I look forward to the report and changes in policy on the watchlist, and, of course, as Secure Flight is implemented, it will be even a better situation.

But anyway, I thank you for what you do every day. Please continue to do it, and we will continue to push you and question.

The record will remain open for 15 days on this hearing for additional statements and questions.

Senator Collins, do you want to add anything?

Senator COLLINS. No. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much.

The hearing is adjourned.

[Whereupon, at 12:06 p.m., the Committee was adjourned.]

THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: INTELLIGENCE REFORM AND INTERAGENCY INTEGRATION

WEDNESDAY, MARCH 17, 2010

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

The Committee met, pursuant to notice, at 10:32 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

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

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. The hearing will come to order. Senator Collins and I apologize that two votes went off that we obviously had to be on the floor for, but we thank you for your patience.

Today, we continue our Committee's inquiry into the intelligence reforms adopted after September 11, 2001. We do so in the fresh context of the failed terrorist attack on Christmas Day, which exposed continuing gaps in our homeland defenses.

Today's hearing, our fourth in this series, will specifically examine the authorities of the Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC). Our purpose is to determine if those authorities are sufficient or in need of additional reform. Creation of the DNI and the NCTC were the most critical recommendations made by the 9/11 Commission to improve our ability to protect the American people against the threat of terrorism.

More than 5 years have passed now since the Intelligence Reform and Terrorism Prevention Act, the so-called 9/11 Commission Act, was signed into law, and that is why last fall our Committee began this series of oversight hearings. The Christmas Day incident only added urgency to our task and underscored, I think, how much this is a continuing effort to strengthen our ability to detect and counter potential terrorist threats.

In recent weeks, we have held hearings on issues raised by the Christmas Day bomber attempt, most recently examining our watchlist and pre-screening systems. Next month, we are going to hold hearings on our visa issuance procedures and intelligence analysis and information sharing. But today, as I said, we are going to focus in on DNI and NCTC. We want to consider instances

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00127 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

in which these two entities have had difficulty carrying out their intended missions as well, of course, as the many times in which they have done exactly what we hoped they would do. We want to discuss also what, if anything, Congress should do to strengthen the abilities of the DNI and NCTC to respond to terrorist and other national security threats, perhaps different threats that have emerged since 2004.

The 9/11 Commission concluded that no single person or agency was in charge of our sprawling intelligence community and therefore recommended creation of the Director of National Intelligence to lead the 16 intelligence agencies of our government, including, of course, the Central Intelligence Agency, and to act as principal adviser to the President on matters of intelligence. The 9/11 Commission Act gave the DNI a range of authorities to better integrate the intelligence community to promote what the 9/11 Commission called the unity of effort that they found was absent before 9/11.

The 9/11 Commission further concluded that no one was responsible for coordinating the critical activities of key agencies involved in the fight against terrorism. As the Commission memorably concluded, no one was in charge of the various efforts that had been ongoing to capture or kill Osama bin Laden.

So the Intelligence Reform Act created the National Counterterrorism Center and gave it the responsibility to conduct a new but critically important function in our government which the statute called Strategic Operational Planning, that is, planning counterterrorism activities on a government-wide basis, integrating all elements of our national power to fight terrorism, and assigning roles and responsibilities to departments and agencies for specific activities based on that planning.

In many instances, the DNI and NCTC have used their authorities very well and implemented critical policies and organizational initiatives to improve intelligence functions and better protect the American people. The NCTC has played a vital role in coordinating Federal, State, and local agencies to prevent an ongoing series of terrorist plots against the United States, including some recent remarkable acts of prevention, including the arrest of Najibullah Zazi and David Headley.

But in other instances, such as the Christmas Day bombing, Umar Farouk Abdulmutallab, failures have occurred in key areas and the progress of fully implementing reforms has been slow, perhaps due to institutional or bureaucratic resistance from some of the 16 agencies that report to the DNI, or perhaps due in other cases simply to insufficient resources or inadequate leadership. Those are the questions that we want to ask today about where there are shortcomings, why they have occurred.

I also want to discuss the policy and legal framework for intelligence community information systems. Last week, the Deputy Director of the NCTC testified that policy, legal, and privacy-related matters impede the development of advanced search and discovery tools that could help analysts spot potential terrorist plots in a way that may have prevented Abdulmutallab from ever boarding that Northwest Flight 253.

This is really a question, as we have discussed after 9/11, everyone concluded that there was an inability to connect the dots, in

part because various intelligence agencies and other agencies of our government were not sharing information and the dots were not on the same table. I think our feeling now is that the dots are on the same table, there is a lot of sharing going on, but there are so many dots on the table that it is hard to many times make the connections that are necessary between them. We are focused now on the capacity of technology to assist us in doing that, because for humans, it is very hard to do it, particularly in a timely way. So I think some of the barriers that were cited last week are ones we have to find a way to overcome in the interest of the homeland security of the American people.

I want to thank the three of you, who each bring very relevant and extensive experience to us, for appearing before the Committee and sharing your perspectives on this, on the issues I have mentioned and others, as well, and I look forward to the discussion after your testimony.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Over the past several months, this Committee has examined the intelligence failures surrounding the attempted terrorist attack on Christmas Day. As part of our due diligence, as the Chairman has indicated, we are also evaluating the impact of the Intelligence Reform and Terrorism Prevention Act of 2004 on our Nation's efforts to combat terrorism.

Today, we focus anew on one of the most significant issues that we grappled with in the drafting of the Intelligence Reform law, and that is the extent of the authority granted to the Office of the Director of National Intelligence (ODNI).

The DNI was established to be, in Secretary Powell's memorable words, the "quarterback" of the intelligence community to coordinate the activities of the 16 intelligence agencies scattered across the Federal Government. Those 16 diverse components carry out an array of missions, and each component has its own view about how best to carry out its assignment.

The intelligence community is resistant to change, but change is precisely what the Intelligence Reform Act directed the DNI to achieve. To that end, we provided a set of authorities that the DNI would use as tools to encourage, cajole, and in some cases compel action. These authorities included the ability to access all intelligence information collected by the Federal Government; the lead role in developing the annual National Intelligence Program budget and in ensuring its effective execution; some ability to transfer funds and personnel within the intelligence community—not as much authority in that area as I would have liked to have seen; the ability to manage and direct the tasking, collection, analysis, production, and dissemination of intelligence; and the authority to develop standards and guidelines to ensure maximum availability of intelligence information within the intelligence community.

These authorities should be largely sufficient for the DNI to accomplish its mission, provided that they are wielded effectively and with the strong support of the President. As Governor Kean and Representative Hamilton testified before this Committee in Janu-

ary, the DNI's ability to lead the intelligence community depends on the President defining the role and giving him the power and authority to act.

The question is, however, whether or not these authorities have been used as often, as effectively, and in the manner that Congress intended. For example, does the institutional resistance of agencies like the Central Intelligence Agency (CIA) make the use of these authorities such an onerous ordeal that the DNI is hesitant to embark upon the journey? Is the DNI concerned that exercising these authorities more aggressively might create ill will that will make it even more difficult to coordinate activities in other areas? Or are these authorities being undercut by insufficient support from the President or the National Security Council, both of which need to be active to ensure that the DNI works as intended?

As the Chairman has indicated, we are also taking a close look at the National Counterterrorism Center. I think that is as important a reform as the creation of the DNI, and I think, as the Chairman has indicated, we have seen great successes from the Center, such as pooling information that led to the Zazi and Headley cases being brought to the attention of law enforcement and the individuals arrested. I do not think that would have happened prior to the creation of the NCTC. On the other hand, we have also seen the NCTC not work as well as intended as in the case of Abdulmutallab.

So our witnesses today offer a great wealth of practical experience in the day-to-day operations of the intelligence community, both pre- and post-reform, and I look forward to hearing their insights on these important questions.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

Senator Collins is right that our three witnesses have been in the system and continue to follow it, so they speak from some experience. In other words, their judgments are informed by experience. One could disagree or agree with them, but they come with some background.

At some point in these deliberations, we are going to speak in open or closed session with some of the people who are running the agencies now, but we thought this would be a very good way to start.

Mr. Powell, we will ask you to testify first, former DNI General Counsel, and currently a partner in the law firm of Wilmer Hale.

TESTIMONY OF HON. BENJAMIN A. POWELL,[1] FORMER GENERAL COUNSEL OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (2006–2009)

Mr. POWELL. Thank you, Senator Lieberman and Senator Collins. I appreciate the opportunity to appear before the Committee to discuss intelligence reform and interagency integration. I am particularly honored to appear before this Committee given the historic role in intelligence reform played by this Committee under the leadership of Senator Lieberman and Senator Collins.

[1] The prepared statement of Mr. Powell with attachments appears in the Appendix on page 359.

I should also note I am honored to appear with Jeff Smith and Ozzie Nelson. Jeff is one of the finest national security lawyers and policy experts in the world on these matters. He is an example to all of us who have worked in this area. Ozzie Nelson is an experienced operator and the Nation is simply safer because of his long service in the military and his work at the National Counterterrorism Center.

I appear before the Committee in my personal capacity and the views I express are my own. I have separately provided the Committee my biography and would refer you to it for my background.

As General Counsel to the first three Directors of National Intelligence, I have seen the implementation of the Intelligence Reform Act at the ground level. And while the work of intelligence transformation and integration can appear quite distant from the daily operational activity of the intelligence community, the September 11, 2011, attacks and subsequent events have made clear that this is work with real-world consequences. The Christmas Day attack was another vivid example of the importance of an integrated intelligence community.

Transformation of the intelligence community is not a zero-sum game. The goal is not to diminish the authorities or the capabilities of one organization in favor of another organization, such as the DNI. The goal is to have an integrated intelligence community that is more than the sum of its parts.

I wanted to briefly highlight three points from my written statement. First, the DNI needs senior-level support to succeed. Second, the DNI initiatives to date have been important, some vital to our security. And finally, since it has been the subject of much discussion over the years, I wanted to briefly touch on the size of the DNI organization.

First, the DNI needs support to succeed. This means support from the senior national security team, the Executive Branch, and the Congress. If he does not have that support and backing, transformation will fail. The reform legislation set up a matrix management structure.

The DNI must be part director, part coordinator, and part diplomat. The Nation has been fortunate to have excellent leaders of the intelligence community, in my experience, both the current leaders and the former leaders, and the Nation is truly blessed that there are brave members of the intelligence community willing to undertake difficult missions around the world at peril to themselves and, at times, their families and their careers. The workforce is talented, mission oriented, and wants to succeed. Our goal should be to give them the tools for success and free them from the ironclad rules of bureaucratic behavior that distract from the one shared goal of protecting our country.

Second, the leadership of the DNI has been absolutely necessary for a number of fundamental initiatives. The DNI did not undertake these initiatives in a vacuum. Their success or failure is dependent on other parts of the intelligence community and the government. But make no mistake, the DNI's Office was the necessary organization, even if not sufficient alone.

Some observers have claimed that the Reform Act and the subsequent implementation merely added another layer of bureaucracy

and accomplished little. That simply does not reflect the reality of the past 5 years. Instead of fairly meaningless charges about another layer of bureaucracy, I would hope that questions would focus on substance, such as are these intelligence community initiatives useful? Historically, how did alternative structures perform? Did they produce the needed integration and transformation of the intelligence community?

Some of the initiatives are discussed in my statement in greater detail. These include reform of the Foreign Intelligence Surveillance Act (FISA), stand-up of the National Counterterrorism Center, implementation of joint duty, security clearance reform, deployment of technologies in innovative ways, such as the Analytic Space and Intellipedia, and critical work in the cyber area that culminated in the Comprehensive National Cyber Security Initiative. This list, of course, omits classified areas that took up significant time and resources of DNI leaders.

A few points: Without a DNI, FISA legislation would not have been enacted. Serious collection gaps would remain and would have worsened and the Nation would face greater risk. Joint duty is critical and its implementation will be a long-term project. It is an example of the investment of time and effort required to formulate and implement workable policies in the intelligence community structure of matrix management.

Security clearance reform: This area has been a particular focus of this Committee's Subcommittee on Oversight and Government Management, the Federal Workforce, and the District of Columbia. The cost and delays present in the security clearance process impose a large cost on the intelligence community and the larger Federal Government.

In November 2005, top secret investigations took 314 days to complete, with only 8 percent being completed in 90 days. I understand that, currently, 90 percent are completed within an average of 91 days. In November 2005, secret and confidential investigations took an average of 153 days, with just 44 percent completed within 90 days. I understand that currently 90 percent are completed within 49 days. I also understand that the decades-old backlog of investigations, which as recently as October 2006 stood at 100,000 cases, has been eliminated.

Without the DNI's Office, the Nation would not have a Comprehensive National Cybersecurity Initiative and be less prepared for the cyber threat that Director Blair recently discussed in his testimony to Congress.

Finally, a quick note on the size of the DNI Office. Director Blair has talked about the DNI's responsibilities for guiding a 200,000-person, $75 billion national enterprise in intelligence. Some facts about the size of the core DNI staff. As of January 2009, Director McConnell spoke in public about a core group of intelligence professionals of 650 people. Under any method of calculation, the DNI is a very small proportion of the entire intelligence community population.

Second, perhaps the proper size of the staff is larger or smaller than the 650 persons that Director McConnell has discussed. I am sure, as with most organizations in government, there are many efficiencies and improvements in staffing that require examination.

But the debate over the right number of personnel pales in significance next to the questions concerning information sharing, collection requirements, multi-billion-dollar acquisition program oversight, analytical excellence, and a host of other issues on the DNI's lengthy list of responsibilities.

Finally, implementation of the matrix management structure created by the Intelligence Reform Act has presented numerous challenges. Many tasks remain undone, and progress on building an integrated, innovative, and more effective intelligence community is likely to be uneven in the coming years. But continued attention on these issues and support for these efforts from the President, the Congress, and senior national security officials is vital if the DNI is to successfully lead the intelligence community into the 21st Century. Thank you.

Chairman LIEBERMAN. Thanks, Mr. Powell. Excellent statement and gets us off to a good beginning.

Next, Jeffrey Smith. We welcome you back to the Committee, back to Congress. We are glad to see you again. Former General Counsel at the CIA and currently a partner at the law firm of Arnold and Porter. Good morning.

TESTIMONY OF HON. JEFFREY H. SMITH,[1] FORMER GENERAL COUNSEL OF THE CENTRAL INTELLIGENCE AGENCY (1995–1996)

Mr. SMITH. Mr. Chairman, it is an honor to be here, and Senator Collins, a treat, as always. I am very pleased this Committee is looking hard at the question of how the statute that created the DNI has worked, and I must be candid. It is not working as well as it should.

To prepare for these hearings, I spoke to many senior intelligence community officers, including in the ODNI. What I found was disturbing and leads me to believe there is an urgent need for a serious in-depth look at the organization and functioning of the American intelligence community.

Congress gave the DNI broad responsibility, but not clear authority to carry out many of these responsibilities. This confusion over authorities lies at the heart of the problem. Senior officials tell me they spend far too much time arguing about these authorities. This creates friction and occasionally anger that distracts from the accomplishment of their important missions. More disturbingly, some officers even speak about mistrust among agencies. That must be addressed.

One of the most prescient observations I heard was that we are slowly replicating the problems of the old DNI. Many believe the dual responsibilities of providing intelligence to the President on the one hand and managing the intelligence community on the other are sufficiently distinct that they should be separated. In a sense, it is the reasoning of the Goldwater-Nichols Act that streamlined the chain of command and clarified that military service chiefs were not to exercise operational control over their services. That responsibility rests with the combatant commanders in the field.

[1] The prepared statement of Mr. Smith appears in the Appendix on page 427.

But all is not gloom. As Mr. Powell said, a lot of good things have been accomplished but problems remain.

I believe the Director's authority should be strengthened in those areas that are essential to the effective management of the community. I think we should focus on two areas in particular: Information sharing and acquisition. I think the Director's authority should be clarified in operational areas where there is some overlap and inconsistency, and that goes to what is his basic role? Is he the strategic adviser to the President on intelligence? Does he do the President's daily brief? Or does he manage the community? Those are two jobs that are full-time jobs in themselves and a lot of people think one person cannot do both.

There is talk about the DNI staff being too large. One problem, I think, is the frustration with the proliferation of contract employees, not government officials who task the agencies. One example illustrates this point. A senior agency official told me that contractors at ODNI had recently requested detailed information about an operation. The agency responded that they were not able to comply with the request because the individuals involved in that operation simply did not have time to set aside the mission and respond to the request. The response from the contractors at ODNI was to offer to send another contractor to the agency in order to answer the questions put by the contractors in the first place. The senior agency official expressed frustration that, to the best of the officer's knowledge, there was not a single government employee in the loop with respect to that particular request.

Now, I have talked to Director Blair about this. He does not seek to micromanage the community or make excessive demands for information. But he points out that there is a mismatch between his responsibilities in the statute and his authority to carry them out, and I agree with Senator Collins. Some of it is the manner in which they are exercised and the support from the President that, as Mr. Powell said, is key.

On information sharing, as this Committee knows, I am privileged to serve on the Markle Task Force, which has spent a lot of time looking at this. I am happy to talk about this in response to your questions. But I think there are some things that can be done with technology in terms of making information more discoverable, adopting an authorized use standard, and permitting data to find data so that we can not only spot the dots that we need, but then we can connect them.

Finally, I think on the issue of privacy, we need some clear privacy guidelines. What I found in my conversations is that there is a lot of uncertainty with respect to U.S. person data, what we can do with it. My privacy colleagues on the Markle Task Force think that the government is being overly cautious in some circumstances, that with this technology, more can be done, but this is a question of guidance and, frankly, leadership and support from the Congress.

Given my role on the Goldwater-Nichols Act when I was on the Senate staff many years ago, you have asked me to think a little bit about how could we have a Goldwater-Nichols Act for the intelligence community. I think there are a lot of things in the Goldwater-Nichols Act that could be adopted, and one of them would be

to streamline the chain of command, to think of the DNI a little bit as the Chairman of the Joint Chiefs and a little bit like the Secretary of Defense. I would also think of the CIA, which is one of the most difficult management issues here, as a combatant command for purposes of providing all-source intelligence to the President and conducting covert operations. If we think of it that way, it helps in my mind a little bit with some of the challenges that we have had with respect to management.

I also think we should think about creating a separate National Intelligence Program. The Administration is taking some steps in that direction, but I encourage them and the Congress to go even further.

Mr. Chairman, I think the time has come to take a fresh look at this statute and I am very pleased that this Committee is asking the hard questions. I think that there ought to be a systematic look at it. It could be done by the Congress. It could be done by the President, using, for example, the President's Intelligence Advisory Board. Or it could be done by an outside group with the support of Congress and the President. I have talked to Congressman Hamilton. As you know, they are very interested in pursuing this. The Kean-Hamilton Commission would be a place to do it. But I think it is important to do it. This is a good opportunity to do it. And I am delighted again to be here this morning and I look forward to answering your questions.

Chairman LIEBERMAN. Thanks, Mr. Smith. Some really provocative things you said, which I look forward to taking up as we discuss what you said.

Next is Richard Nelson, who is known as Ozzie.

How many people in the room remember Ozzie and Harriet? You see, we are limited now. [Laughter.]

I should ask how many remember Ricky. Maybe that would be better. [Laughter.]

Anyway, to return to the seriousness of the moment, Mr. Nelson is a former official in the National Counterterrorism Center's Strategic Operational Planning Directorate. He is a retired Navy officer and currently is the Director of the Homeland Security and Counterterrorism Program at the Center for Strategic and International Studies here in Washington. Thank you for being here this morning.

TESTIMONY OF RICHARD NELSON,[1] SENIOR FELLOW AND DIRECTOR, HOMELAND SECURITY AND COUNTERTERRORISM PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. NELSON. Chairman Lieberman and Ranking Member Collins, and distinguished Members of the Committee, thank you for the opportunity to discuss this important topic. I am not sure if it is good or bad to go after the lawyers, but I appreciate the opportunity to testify with them. [Laughter.]

I was one of the inaugural planners assigned to direct strategic operational planning, so today, I am going to focus my remarks on NCTC and its legislatively role, mandated role in that capacity.

[1] The prepared statement of Mr. Nelson appears in the Appendix on page 445.

The Intelligence Reform and Terrorist Prevention Act (IRTPA) addressed some serious weaknesses in our Nation's intelligence community and its ability to combat terrorism. In creating the DNI and the NCTC, the landmark legislation sought to improve collaboration among numerous departments and agencies that deal with our threats to our Nation's security. Among the Act's most significant contributions was its recognition that our Nation's Cold War national security organization was no longer sufficient to address the complex and myriad transnational threats we face today in the 21st Century.

As with any innovative idea, achieving the aims of legislation will come through evolution. Valuable lessons can and should be learned when ideas and concepts meet implementation. Those lessons should be leveraged to improve upon the original ideas and ensure the vision of its creators is being met. This is the case with NCTC and particularly with the Directorate of Strategic Operational Planning (DSOP).

Why do we need a stronger and more effective DSOP? In short, while numerous departments and agencies work aggressively to counter threats as they emerge, the intelligence community, and arguably the government as a whole, still lacks a truly interactive process for addressing terrorism. One need look no further than the failure to "connect the dots" on December 25 to understand why coordination is so important.

Furthermore, because so much of the effort is channeled toward the immediate exigencies of the day, the government has not devoted sufficient long-term thinking to how to develop a common and ultimately strategic framework for dealing with terrorism and other threats. This has become only more important as we move forward and coordination with State and local governments becomes more critical and the lines between the private and public sector continue to blur.

Elements of DSOP must be addressed in three key areas: Mission, authorities, and personnel. DSOP's mission must be refocused to ensure its role in and value to the interagency counterterrorism architecture is understood. DSOP was given the broad guidance to conduct strategic operational planning. The intent was for DSOP to fill the void in counterterrorism planning between strategic level policy making and tactical level operational activities.

To attempt to close this gap, the term Strategic Operational Planning was created and tasked to DSOP. The conflating of these terms, strategic and operational, has hindered DSOP since its inception and remains a significant problem. These are terms of art, and those with background in planning understand clearly that they are separate and unique requirements. By merging these terms, DSOP is stranded in what I call a planned no man's land between high-level policy and strategy development and operational and tactical-level planning.

We have a chance to refocus DSOP's mission before it becomes ingrained and irreversible and I recommend that we split it into two distinct branches, one that focuses on strategic and one that focuses on operational. The strategic part should focus on high-level counterterrorism policy, strategy, and resource allocation. It should lead interagency policy and strategy making, including ef-

forts that require White House approval. The element should also have an enhanced and a more assertive role in resource allocation and drive the input to the Office of Management and Budget (OMB) to resource counterterrorism prioritization investments. While this mandate currently exists, DSOP's role should be strengthened and enhanced to ensure that requirements are tied to strategic outcomes.

A second part of DSOP should focus on operational plans against terrorist groups. Such a construct provides attainable goals: Defeat of a group. The National Implementation Plan should be amended so that it can be executed geographically. Whether justifiable or not, the Cold War-based security infrastructure executes geographically and not functionally.

Authorities—the IRTPA gave the DSOP the authorities to conduct its specific mission, yet no authorities were taken from any other department or agency in support of DSOP's creation. Not only does this create overlapping authorities, but it established no compelling reason for departments or agencies to participate in the DSOP process, as they could continue their counterterrorism efforts under extant power. These overlapping areas of responsibility must be clarified. Without this, departments and agencies will continue to spend time fighting turf battles when they should be focused on the enemy at hand.

The question of authorities is raised regularly in discussions regarding DSOP. The recent Project on National Security Reform Study offers a comprehensive assessment of this issue. A comparison of authorities between the Office of Drug Control Policy, DNI, and DSOP, three organizations chartered with similar tasks, highlights the disadvantage from which DSOP operates and notes that DSOP is the only entity of the three without authority over people or money.

Many cite DSOP's explicit prohibition from directing operations as a key reason for its struggles, while some call for empowering DSOP with additional authorities in this area. This should not be done, as DSOP lacks the capability and capacity to assume such a role and would fall far short of expectation. With no authority over personnel, resources or operations, DSOP has a limited ability to compel interagency participation and thus remains a relatively powerless organization. It also relegates DSOP to the unenviable role, of leading process-oriented approaches to substantive problems. Departments and agencies that actually control operations, personnel, and resources address substantive counterterrorism problems under their own authorities.

To solve this problem, the authorities issue must be addressed across the entire government counterterrorism enterprise. Specific to DSOP, it should be given authority to influence both resources and personnel.

In personnel, DSOP should be given the personnel to conduct its mission. The issue of personnel remains a significant factor limiting the evolution and ultimate effectiveness of DSOP. To succeed, NCTC must have the right talent. A clear mission with ample authority rings hollow if the appropriate personnel are not brought together to execute what is required.

DSOP has been hindered by a lack of planning talent since its inception, and unlike its analytic and knowledge management counterparts in NCTC, no standing cadre of interagency counterterrorism planners existed from which a terrorism-specific capability could be created.

While the process of building a capacity has begun, it has been slowed by two key factors: The lack of interagency participation and high personnel turnover. First, the interagency must become fully invested in NCTC and DSOP concepts. By being fully invested, it includes not only recognizing and embracing DSOP's mission, but also detailing the appropriate number and type of personnel and ensuring robust participating in the planning. The old adage that plans are nothing and planning is everything is only valid when those that are conducting the planning are actually involved in the execution of those plans. Since DSOP does not execute plans, it is imperative that its efforts include robust participation by the departments and agencies.

Participation in interagency planning efforts such as DSOP must be made part of the government intelligence community human capital system. Personnel, particularly those with operational experience, must be rewarded through pay and promotion to incentivize service in such entities as DSOP.

And second, personnel turnover at DSOP must be limited. This will occur, in part, by changing perceptions regarding the value and credibility of DSOP, but we also must establish a standing career pipeline for interagency counterterrorism planners. This will incentivize talent to pursue careers interagency.

I have submitted more comprehensive remarks for the record, and again, I appreciate the opportunity to speak today and I look forward to your questions.

Chairman LIEBERMAN. Thanks very much, Mr. Nelson. That was really interesting.

As I listened to the testimony, particularly of yours—Senator Collins probably had the same reaction—I can remember the extensive debates about the various terms that we put into the 9/11 Commission legislation. It is almost as if, but not quite as neat, that we were architects or a construction management operation deciding how best to build a building. And not as neat because there were more interests at the table than the design-construction teams, because in some sense, the people at the table wanted to preserve the existing parts of their building. But anyway, having gone through that self-analysis, I will thank you for your testimony and we will begin the questions with 7-minute rounds.

Mr. Powell, let me go to the first point you made, which is the importance of senior-level support, government-level support, for the Director of National Intelligence for the position to succeed. I think that is a very important and strong point. This is not the kind of thing you put in a statute or has to happen, but we are creating something new. It has new supervisory authority and the natural inclination of agencies to resist any losses in their own autonomy.

So from the unique perspective you have had, would you say that the DNI has received, since the creation of the office, the support

that it needs from the two Administrations under which it has now begun to function?

Mr. POWELL. Yes. Thank you for the question, Chairman Lieberman. It is a critical question, as I mentioned in my statement. Although I did serve some number of months in the current Administration, obviously, I can speak most directly to the former Administration, and as I noted in my written statement, some myths about the founding of the DNI and former President Bush's support for the DNI. Whatever happened in the summer of 2004 and whatever different testimony was coming from the Administration, I do know where former President Bush ultimately came down on the issue, and where he came down in December 2004, and I observed most directly in discussions——

Chairman LIEBERMAN. And how would you describe——

Mr. POWELL [continuing]. His support for the DNI——

Chairman LIEBERMAN. He supported it, yes.

Mr. POWELL. Well, in a number of ways. There was discussion about whether or not the DNI needed to be in the Oval Office as part of the briefing team. And I think that there was a feeling among the senior national security team that given some questions about the matrix structure that was set up, that it was important from an intelligence perspective, but it was important as a message to the Administration and to the senior leaders of the intelligence community that this was the person who the President was counting on to lead an integrated intelligence community.

When you look at these initiatives, the Foreign Intelligence Surveillance Act, Executive Order 12333, the work in the cyber area, and any number of initiatives, those depended not just on the DNI making a decision, but having the backing of the President to make that decision.

Executive Order 12333 is a bit obscure to people out in the public, but it is the foundational Executive Order that was signed in 1981. It was very out of date. It was not applicable to the current intelligence community that we had in terms of its organization, particularly post the Intelligence Reform Act. Why had it not been updated since 1981? Endless attempts to update it failed because of interagency disagreement. So it is an example. In that one, the former President had to bring that to a close.

Chairman LIEBERMAN. Yes.

Mr. POWELL. There were issues that had to go to the former President and he had to rule on them. So it is just absolutely vital. I mean, it is vital for any department head——

Chairman LIEBERMAN. Sure.

Mr. POWELL [continuing]. To have direct control and authority over everyone in their department. If they do not have the backing of the President, they have trouble succeeding. In a matrix management structure like the DNI, it becomes even more critical.

My experience, although limited in the current Administration, seemed to be supportive of intelligence transformation, where it was going. But again, I can really only speak until essentially the beginning of March 2009, from an insider perspective.

Chairman LIEBERMAN. Right. So your impression from outside has been that the current Administration has continued that support of the DNI?

Mr. POWELL. Well, I hesitate, because most of my information is just based on press accounts, and having been on the inside, I hesitate to rely on press accounts.

Chairman LIEBERMAN. Yes.

Mr. POWELL. I mean, I think it has been challenging. The Administration has had a lot on its plate. They have had a lot of other very important priorities, obviously things completely different—health care, a number of issues that are on the plate. But every President has a lot of issues at the same time on their plate.

I guess I would say that I think the Christmas Day attack has brought it into greater focus, the importance of these issues. It is one thing to understand how important they are and to understand how the country is at threat. It is another thing when you actually have a situation that was, frankly, minutes away from there being 300 empty chairs at the dinner table that evening in Americans' homes. So I think that brings a greater urgency and a focus in a way that talking about the threat simply can not. So I think you have seen renewed focus on it and it is fortunate that event was not successful.

Chairman LIEBERMAN. Agreed. Mr. Smith, let me ask you to pick up there and go to the most public, not necessarily the most important, but the most public manifestation of this question of not only where the White House is in backing the DNI, but how the DNI has merged with other agencies of our government.

I will tell you that when we were struggling to put the DNI together in the legislative process, the greatest push and pull of the people around the table was from, frankly, people representing the Department of Defense worried about incursions that the DNI might make. In fact, perhaps that has not been a problem in implementation. Some of that may be because the simple twist of fate that Bob Gates, a former leader in the intelligence community, turns out to be the Secretary of Defense and it works out better.

But there seems—not that we were naive about the potential for tensions within the intelligence community with a new overseer, but look, I am speaking about the public blowup over whether the DNI would have the authority—and this was last year—to appoint senior intelligence officials in foreign countries with the CIA, and the public impression is that the DNI lost that fight. I wanted you, to the extent that you want to get into that fight, welcome that, but take off from it to the larger question of whether, in your opinion, the national leadership in both Administrations has supported the DNI, and two, about the extent to which there remain tensions between components of the intelligence community and the Director of National Intelligence.

Mr. SMITH. That gets to the heart of the issue, Mr. Chairman, and I am glad you raised it. With respect to the particular dispute over the DNI's authority to appoint his representative overseas——

Chairman LIEBERMAN. Right.

Mr. SMITH [continuing]. I think it is deeply unfortunate that it had to be referred to the White House. I think everybody involved now would have preferred that to have been worked out internally, but that was not the case, and I can only imagine that the people at the White House did not enjoy having to referee this dispute. Nevertheless, I think the decision by the President was to split the

issue a little bit. In some respects, the DNI won, and in some respects, the Director of the Central Intelligence Agency won.

But in general, my impression from talking to senior people, including people in the White House, is that there is no doubt that this President supports a strong DNI. They also wish to deal directly with the CIA on those matters for which the CIA is responsible, and I think that is understandable. The CIA is the operational arm of much of the intelligence community. It conducts covert operations, which are very important to the President. It is the only agency that is still "central," and is largely responsible for production of all-source intelligence.

So I think we have to recognize that fact and find a way to give the DNI the authority that he or she needs to manage the agency, to manage the community, but without interfering with this relationship between the President and the CIA. And that is why the notion of a combatant command appeals to me, because the President deals directly with General Petraeus, as he should, and yet the Chairman of the Joint Chiefs and the Secretary of Defense are very much involved in that conversation, and we have been able to work out those relationships in the Defense Department. We ought to be able to do it in the intelligence community.

One more thought, Mr. Chairman, on your point about the defense agencies.

Chairman LIEBERMAN. Yes.

Mr. SMITH. It has worked out for a variety of reasons, including the fact that we have men occupying these positions who have worked together in the past who have strong military backgrounds. Another element is that we are at war, and when that happens, a lot of the issues kind of fall to one side, and within the military, we find a way to work these problems.

There is another concern I heard expressed, which was that the role of the Defense Department and the role of supporting the warfighters among these defense agencies is now so dominant that there are some, including in the military, who worry that they may have drifted a little bit from their national mission, that is to say, broader support of foreign policy. What is happening in those areas of the world that we care about beyond just Iraq, Afghanistan, and al-Qaeda? So these are issues, again, that we need to look at and be alert to.

Chairman LIEBERMAN. That is very helpful. Thanks. My time is more than up, but I look forward to continuing in the next round. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I, too, had flashbacks as I was hearing Mr. Nelson's testimony and reading your testimony, Mr. Smith, about the abrogation word, which I so remember in December of that year, calling Senator Lieberman after my Chief Counsel came up with the word "to abrogate" as being the way to stop the House Armed Services Committee from sinking the entire bill. So a lot of the issues that you have raised have a complicated history, and without some of those admittedly awkward compromises, we never would have gotten a bill through. It was an extraordinarily difficult achievement but an important one.

I want to talk about information sharing. Last week at our hearing, the Deputy Director of the NCTC surprised me, at least, by saying that there was limited ability for the intelligence community to search for information across the many databases maintained by intelligence and law enforcement communities, and those of us who have used Google every day and put in names that were not spelled right and then Goggle tells us, "Did you mean X," were really surprised to learn that a misspelling flummoxed the search on Abdulmutallab at one point in the information systems.

The Deputy Director, however, was very emphatic in warning us that there was no silver technological bullet, and that was at odds with a lot of presentations that our staffs have had on this issue and the work that you have done, Mr. Smith, on the Markle Foundation, which I think has been terrific work, that you and Zoe Baird and others have done. He said, "notions of a Google-like search or a federated search are actually of relatively limited value due to legal, policy, and privacy issues." And I would like to get a better understanding of what those barriers are, because it is really troubling to me that we cannot design a system that respects privacy concerns—which I care deeply about—and yet does not prevent us from accessing information.

So, Mr. Smith, I am going to start with you, and then Mr. Powell and Mr. Nelson, I would like to hear your views, as well.

Mr. SMITH. Senator, you put your finger on a really critical issue. We were a little surprised to hear Mr. Travers' testimony, and so actually Mr. Powell and I met with him on Monday afternoon to talk about this in a little bit of detail and we have talked about it within the Markle Task Force, because we, too, wanted to drill down and understand what he said.

Some of it, I think, may touch on some classified information and some classified systems, so I want to be a little bit careful here, but clearly, with respect to getting access to databases outside of the intelligence community in some of the other departments, some of these lists and so on, he has felt that he has not been able to reach into databases, particularly in the Department of Homeland Security and other places, where he would like to be able to have his analysts reach in.

In the Markle Task Force, we think that there is technology that would permit that and protect privacy at the same time. So we intend to spend a little bit more time on this. Mr. Travers has been extraordinarily generous with his time with us and we are going to get some of our technical people, as well, involved to see if we cannot craft a solution that can get at this because as a matter of principle and policy, we believe that privacy can indeed be enhanced by these technologies because of things like anonymization and authorized use. We think this is an important issue and we are going to continue to work on it. We look forward to working with this Committee.

Senator COLLINS. Thank you. Mr. Powell.

Mr. POWELL. It is an absolutely critical question, Senator Collins. Let me discuss it from the perspective of trying to lay out a little bit of the issues that are faced by NCTC and faced by us in the DNI's Office in trying to obtain data sets for NCTC. As I talk about in my statement, at NCTC, since its stand-up, we have put over

30 different networks—military, law enforcement, and other types of networks—into NCTC with data sets that exceed that number being accessible to NCTC.

I think the Committee would want to think about examining a couple of different areas. First, you would want to look at the Memorandum of Agreement between the Attorney General and the Director of National Intelligence on the search, use, retention, and dissemination of data sets containing terrorism and non-terrorism information, or information exclusively pertaining to domestic terrorism. Now, that is a mouthful, and what does it mean in practice?

Those guidelines lay out three primary areas in which NCTC can get access to data sets that contain non-terrorism information, and let me be very specific about examples of what I am talking about. Here, I am talking about data that may be obtained by DHS or other agencies that is not acquired from people who are known or suspected or even that there is any reasonable suspicion of terrorism activity in there. So basically, you are talking about information from Americans and non-Americans that are obtained for travel or other reasons. They are not obtained because these people have no suspicion about them.

That agreement is going to set out three ways that NCTC can access data. One, account-based access, so think of that as you go to a terminal, log in, do your search, log off, and then go back to your terminal.

Two, search and retention, and what I mean by that is that I give a search to the data set owner, so think of it as, for a hypothetical, DHS. They do the search in a batch or some other method and then they give me the results.

Finally, the third area, and that is called data set replication, and what we are talking about there is actually ingesting the data into NCTC. That is perhaps the most effective way, which allows that Google search capability. What you will find in those guidelines is you will only be allowed to do data set replication if, for some reason, account-based access or the search and retention areas do not work.

So what does that mean in practice? I guess the best way to describe it is when you do a Google search on your computer, it goes out and searches the Internet and returns your results from the Internet. Depending on your settings, it probably does not search Committee databases or Senate databases that are internal to the Senate, nor does it search your individual offices' databases. So Google, itself, is not a true federated search that searches all of the information technology systems that you are connected to.

So there is, in my experience, Google-like search capability at NCTC. The problem is the number of data sets that it is allowed to touch. So we have this Memorandum of Agreement that lays out for Fourth Amendment and privacy concerns with this different criteria of access.

Two other areas that are absolutely critical when thinking about this. This data was obtained under specific agreements and arrangements. Each one of those databases needs to be taken on its own terms, and there may be restrictions associated with them

that were the only reason we are able to get that data. So it is a little bit like the reform legislation. Compromise is entailed.

There has been a lot of public discussion about European PNR data and what the arrangements are at the diplomatic level between the United States and Europe, and there were agreements made and those agreements, frankly, have consequences throughout the government for accessing that data. There has been public talk in the area of financial terrorism information and general financial information and agreements placed in those areas.

Finally, the FISA Court. You cannot go out and grab unminimized FISA data. There are FISA minimization guidelines that require the data be minimized according to FISA guidelines before it is given to NCTC and be made available for anyone to search.

So these are some of the practical things I think you would want to look at at a baseline level when you are looking at this. We spent a lot of time looking at the U.S. person guidelines across the agencies to see if we could make them more uniform. It is a slog to go through them.

Senator COLLINS. Thank you. Mr. Nelson.

Mr. NELSON. Senator Collins, thank you for that question. Regarding information sharing, we are never going to have perfect information sharing, but we need to continue to do better. In my operational experience, it was always a source of frustration to me: The amount of data, the number of systems, and people trying to bring it all together. It was always astronomical, and very challenging.

And I also think we have to overcome this culture of secrecy, as I call it, in the intelligence community. Certainly, it is important and it has its place, but it continues to prohibit information sharing especially when individuals with the same clearance level will not share information because there is not a need to know, which is determined by the individual who actually knows the information. I do not know how some assessments like that can be made.

But why the information sharing piece is even more important, and I cannot talk too much about the civil liberties part, not being a lawyer, is that the Federal part of this is the relatively easy part. We are going to have to come up with ways to share information better with our allies, which is still a huge weakness. And better ways to share it with State and local governments, especially as we deal with issues such as homegrown extremism, which has been in the media recently, and with the private sector. When 85 percent of the infrastructure is owned by the private sector, we are going to have to overcome information sharing obstacles. It is going to be so critical that we accelerate the use of technology at the Federal level because the problem is only going to get worse when we have to share with other folks. Thank you.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Carper, good morning.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Good morning. Looking at this sea of green, it is like a puddle of green, would not you say? Maybe some folks did

not get the memo, but it is nice to be with all of you on St. Patrick's Day.

To our panel, welcome. Thank you for joining us.

In my own view, the Intelligence Reform and Terrorism Prevention Act that we adopted about a half-dozen or so years ago has done a fairly good job of streamlining the intelligence community's command and control authorities. With this Act, all of the Federal Government's various intelligence entities report to the Director of National Intelligence, as you know. And so while the organization has improved, I think, I hear there remains a serious turf battle—we talked a little bit about that here today—between the Directorate of National Intelligence and the Central Intelligence Agency. One example of that is between the CIA's Directorate of Intelligence and the National Counterterrorism Center analysts when presenting intelligence issues to the rest of the Federal Government.

I would just ask if each of you could take a minute or so and just comment on this particular turf issue. Let me know if you agree with those observations and share with us any recommendations you might have for our Committee, how to deal with it.

Mr. Nelson, why don't you lead off.

Mr. NELSON. Thank you, Senator. I appreciate the question. I am not an analyst by trade, so I will just keep my comments brief. I will say my personal assessment is the NCTC is one of the areas of the ODNI which I think has been extraordinarily successful, and I think that they have actually been producing some significant work and have made major improvements along those lines.

But as far as comparing it to the agencies, I would have to defer to my colleagues here. Thank you.

Senator CARPER. All right. Thank you.

He is passing the buck to you. What do you all have to say?

Mr. SMITH. I am a little bit like Mr. Nelson. I do not have——

Senator CARPER. You are going to put a lot of pressure on Mr. Powell. [Laughter.]

Mr. SMITH. Well, with respect to the critical question of analytical support to counterterrorism, in preparing for these hearings, I talked to a lot of people and that issue did not surface, interestingly enough. It may be an issue, but it was not raised in my conversations.

However, there were a lot of other concerns raised that I talked about in my prepared remarks, namely there is a lot of tension within the intelligence community over the issue of authorities. And in my judgment, senior officials spend far too much time arguing about authorities. Some of that is an inevitable result of the way the intelligence community worked in the past, compromises made in the legislation to get it adopted, and I understand the importance of that. But my suggestion has been that this is a time to take a look at those authorities. We have had 5 years of experience. We know what works, what does not work, and see if we cannot adjust those and enhance the ability of the DNI to manage the intelligence community and at the same time enhance the capacity of the individual agencies to function more effectively.

So there are some problems and I am pleased this Committee is looking at them.

Senator CARPER. Well, good. You did not answer the question I asked, but that was a pretty good answer. Thank you.

Mr. SMITH. Well, I beg your pardon. I am happy to try again, sir.

Senator CARPER. No, that was good. Thanks. That was helpful. Mr. Powell.

Mr. POWELL. Senator Carper, this is a critical issue which I dealt with extensively. I think it is far better than it was. When the DNI was initially stood up, there was considerable frustration on two counts, I think, at the senior levels. One, that the President himself personally remained the integrator between foreign and domestic intelligence, and I did not think that was a role for the President, for the foreign threats and the domestic threats to be landing in the Oval Office for everyone to have that discussion right there. I thought the President deserved better.

There were still exactly what you pointed out, difficulties in lanes of the road of different organizations producing their own version and take on urgent threats to the Nation in the counterterrorism area. I believe in diverse intelligence and diverse views. I do not believe in giving different factual scenarios to the President. I think we should be able to get our facts together.

So there was a lot of effort and lanes in the road. Who produces homeland threat reports? Who has the responsibility for putting out the alerts, for putting out the senior briefings, for kind of getting the global picture? You now have, of course, three times a day, the secure video-teleconferences run by NCTC. You had some initial issues on resources, both the CIA Directorate of Intelligence and the NCTC need to have al-Qaeda analysts and people who speak the language and can take a longer-term view of things. There were some transfers of personnel made over some not inconsiderable public and private controversy.

Admiral Redd, the Director of NCTC at the time, came up with lanes in the road documents about who was going to do what. I mean, you could argue about the decisions made in those lanes of the road. I think it is a lot better than it was. I do not hear as often today about the problems, and it may reflect that I would not because so much of it is classified, where different agencies are duplicating the same work unnecessarily.

So I think the lanes in the road are far better worked out than they once were. It may be that there is some still duplication out there, but we spent a lot of time, a lot of meetings, a lot of debates about who exactly was producing the picture for the national security team and the Congress.

Senator CARPER. Thank you. One more question, if I could.

Chairman LIEBERMAN. Go right ahead.

Senator CARPER. Thank you. I believe each of our witnesses today are in the private sector now, is that correct?

Mr. POWELL. Yes.

Mr. SMITH. Yes.

Mr. NELSON. Yes.

Senator CARPER. All right. And in part as a result, I think you are maybe better able to present a unique perspective and to speak with candor about the current Administration's counterterrorism policies. You have done this already in part in your testimonies, but I am going to ask you to come back to this again—I was won-

dering if you all could take a moment to share with us how things have changed since your Federal Government experience, and based upon current events, such as the shootings at Fort Hood and the attempted Christmas Day bombing last year, just briefly discuss some steps that the intelligence community ought to be doing to close the intelligence gaps we have been talking about over the course of the last several months.

Mr. POWELL. I can go first. Thank you for the question, Senator Carper. I have reflected a lot on this subject. I mentioned to Chairman Lieberman earlier that I think the attempted Christmas Day bombing of the jetliner brought the issues I talked about in the statement and that we are talking about today a new urgency and a focus. I think, for good or bad, we were very seized with the issue on a daily basis, and obviously the former President, having been through September 11, 2001, was very seized with the issue and made it an extremely high priority. We could discuss whether that was too high a priority or whether that was good or bad, but as a result of that, the intelligence community and the DNI, I would say, occupied a very central place at the table and these issues were very central on the Administration's agenda.

Obviously, this Administration, President Obama has talked about how critical it is, how important it is, but there is a lot going on and some of these issues take time and you need to work through them.

What I have observed, at least through the press and talking with people, is a new urgency and focus as a result of the Christmas Day bombing, really bringing home—when you are discussing whether or not NCTC can get access to a database, when you need the Attorney General to change some guidelines to enable an intelligence operation or to enable some information sharing to happen. It is far less academic, I think, post-Christmas Day bombing than perhaps I noticed before.

There are some issues that I would probably differ with some decisions that were made that I think have perhaps caused some difficulty for the intelligence community. They were made for global and diplomatic and reasons that I think the President and the Administration felt very strongly about. I think they have had impacts on the intelligence community, and that is just a byproduct of those decisions. They may have been the right ones overall for the country, but they have had some negative impacts on the intelligence community.

Senator CARPER. My time has expired. Mr. Chairman, should I yield back?

Chairman LIEBERMAN. I think you have no time to yield.

Senator CARPER. That is fair enough. Mr. Smith, Mr. Nelson, each of you, thank you for your testimony today.

Chairman LIEBERMAN. Thanks, Senator Carper.

Senator CARPER. I will come back another day for that question.

Chairman LIEBERMAN. Thank you. Mr. Smith, you said some things at the outset of your opening statement which are really important, which is the general statement that the DNI statute, in your opinion, is not working as well as it should, and that is disturbing, that is the word you used, and I agree. And the general statement you made was that the Office of the Director of National

Intelligence has broad responsibility, but not clear authority. You called on us then to strengthen the statute.

And I know you have invited a process, either within this Committee or the Foreign Intelligence Advisory Board or perhaps some outside group. But talk a bit, if you can, about where you would begin to strengthen the authority of the DNI.

Mr. SMITH. I think it is largely on the management side, Mr. Chairman. The two or three areas that I looked at in preparing for this were, one, information sharing, and we have talked about that and I think there does need to be some strengthening of authorities and/or clarification of those authorities, particularly with respect to privacy.

A second area is the acquisition area. There is confusion over some areas, particularly on independent cost estimates, who is responsible for them and so on. Now, some of that is in the legislation, but what I have discovered is there is still some confusion, namely; is it yours, is it mine, who is responsible?

A related area is reprogramming. Again, there is some uncertainty there. The House and Senate intelligence authorization bills have, as I understand it, some language to try to clarify that, but that is an indication, and when I talked to the staffs of the various agencies, they would tell me, well, there is a big fight going on right now about some issue or another, most of which could be traced to some uncertainty in these authorities. Now, these are men and women of goodwill. They really want to do the right job. We should all be proud of how hard they are working and how dedicated they are to doing it.

Chairman LIEBERMAN. Agreed.

Mr. SMITH. But the flip side of doing that is they are very proud of what their responsibilities are and their organization and they tend to think it is my responsibility, let me do it. So as a general matter, I think there are maybe a half-a-dozen or so areas where I would begin to concentrate.

Chairman LIEBERMAN. Would you add to the budget authority?

Mr. SMITH. Yes, I would. I think that serious consideration should be given to further separating the National Intelligence Program, and that includes some budgetary authority. Now, the DNI does have, and Mr. Powell is better able to speak to this than I am, some budgetary authority over the authorization of budget.

Chairman LIEBERMAN. Right.

Mr. SMITH. And it goes to Senator Collins' point earlier about whether that authority has been used, and the risk of having authority that you either do not use or try to use is then it gets taken away from you through some other process. In my conversations, it has gotten better over the last 2 or 3 years. That is in part because of personalities and in part because of some leadership from the White House and DOD that says, look, we should not be having these fights.

But the statutory language remains, and as long as some of that uncertainty is there, another set of leaders might not be quite so accommodating. Both, by the way, in the previous Administration and in this Administration, I think there has been a lot of progress. So I would like to have a situation that is less personality-depend-

ent and where the authorities line up a little bit more with the responsibilities.

Chairman LIEBERMAN. Let me ask you, continuing in this focus, on a particular idea you raised in your testimony, which is to separate the DNI as the manager of the intelligence community from the role that was also given to the DNI under the statute, which is as essentially the chief advisor on intelligence to the President, and therefore responsible for the daily briefing to the President. I mean, the argument then, to a certain extent, repeated by Mr. Powell this morning in terms of judgments that were made early on by President Bush, is that unless the DNI is in there every morning with the President, that he does not have the stature. So weigh the balances here and why you think it is still a better idea to separate those two functions.

Mr. SMITH. This is not to say, Mr. Chairman, that the DNI should not be in the room with the President during the briefing. Perhaps not every day, but certainly be there.

Chairman LIEBERMAN. Right.

Mr. SMITH. The question is whether or not the DNI has the responsibility not simply to be there, but be the person who is actually directly and personally responsible for preparing it, giving it, following it up, and so on. And I do not know how it is presently working. Let me be very clear about that. But the concern I have heard expressed is that different DNIs have done it differently. Different Presidents want it done differently. But the fact of the matter is that the responsibility of personally briefing the President and, as you know, the President's Daily Brief (PDB) is also seen by other senior cabinet officers——

Chairman LIEBERMAN. Right.

Mr. SMITH [continuing]. That responsibility is so huge and the follow-up to those discussions is so huge and the participation in the policy-level discussions about what to do is so huge that no single individual can do that and effectively manage the community. And that is why what appealed to me was beginning to think of it a little bit as we had done in the Goldwater-Nichols Act, which is to separate the operational responsibilities to actually do the warfighting in the field from the responsibility to train, equip, and maintain the forces that are then assigned to the combatant commanders in the field.

It is by no means a perfect analogy and I am not sure it lends itself necessarily to statute. But nevertheless, one hears that perhaps DNIs, and this may be as a result of the way the President wants to do it, but if that is going to take the majority of their time—it is a hugely important responsibility—that means that necessarily there is less time to devote to management. So that is an area where I think people need to give some serious thought as to what that balance is, what the authority should be, and what the law should be.

Chairman LIEBERMAN. I understand it better. Incidentally, I think the Goldwater-Nichols strategy is a helpful one and one that we will think about.

So as you have thought about this question—I understand what you are saying. The responsibility for the daily briefing of the President is a big one, and I presume takes the time of the DNI

to get ready and to follow up. But if the DNI did not do it, who would do it in the best of all worlds, as you see it?

Mr. SMITH. In the past, the practice had been that there was a senior—this was before the DNI was created——

Chairman LIEBERMAN. Yes.

Mr. SMITH [continuing]. There was a very senior intelligence officer from the CIA——

Chairman LIEBERMAN. But not the Director of the CIA.

Mr. SMITH. Not the Director. Now, the Director would occasionally go, but it was on occasion, just to sort of be there——

Chairman LIEBERMAN. Right.

Mr. SMITH [continuing]. Or where a particular subject would come up. But there was a whole PDB staff. There was a whole bureaucracy that had grown up. When I was at the agency, there were meetings where we would decide what went in the PDB. Different agencies would make presentations.

Chairman LIEBERMAN. And the Director would have some part in that, I assume.

Mr. SMITH. Very little.

Chairman LIEBERMAN. Very little.

Mr. SMITH. It was the senior analysts that did it. I have even heard some concern expressed, Mr. Chairman—I have no personal knowledge of this, but there is some concern that as you try to bring more agencies into the production of the PDB, the advice a President is getting begins to look a little bit like the advice that the President got prior to Goldwater-Nichols from the Joint Staff, which was the least common denominator where it is a committee product——

Chairman LIEBERMAN. Right.

Mr. SMITH [continuing]. Which is another reason I am attracted to the idea of having the CIA and/or the National Intelligence Council (NIC), be the combatant command with a very direct responsibility to the President, like General Petraeus, to do that mission.

Chairman LIEBERMAN. Right.

Mr. SMITH. And they are ultimately in charge of deciding that. Now, the DNI has to make sure that, ultimately, he or she has a voice in that, but it is a huge responsibility and I understand DNIs are too frequently drawn into that.

Chairman LIEBERMAN. So I am going to wind this up, but just by saying it sounds to me that what you might prefer here is that some senior person in the Office of the DNI——

Mr. SMITH. Yes.

Chairman LIEBERMAN [continuing]. Handle the presidential daily briefing.

Mr. SMITH. That is correct.

Chairman LIEBERMAN. Thanks very much. Senator Collins.

Senator COLLINS. Thank you.

I want to make just one comment on the information sharing before leaving that issue and before going on to another question. Mr. Powell was going through the various restrictions, some from the Attorney General's guidelines, some from memoranda of understanding that were worked out to get information, some from FISA Court decisions. So obviously, this is complex. But what that tells

me is some of the restrictions are the result of law, some of them are the result of policy choices, some of them are the result of negotiations in order to get information. Mr. Powell, just quickly, is that generally a fair assessment?

Mr. POWELL. Correct, Senator Collins.

Senator COLLINS. So I really want to work with you after this hearing to better identify a solution. I think both the Chairman and I, at the risk of speaking for the Chairman, were alarmed when we heard the testimony that we did from the NCTC Deputy Director because it certainly seems to be interfering with accessing information that needs to be accessed, and I think, Mr. Smith, your point that you can design systems that actually enhance privacy while allowing this access is absolutely a critical point.

I want to move on to the relationship between the DNI and the CIA. We have talked previously in this hearing about the friction between the two, the White House having to get involved in resolving disputes. That really concerns me when it gets to that level. But there has also been this, I would call it an urban myth in some ways, that the Intelligence Reform Act did not define that relationship, and Mr. Smith, you referred to it in your written testimony. To me, it is just so crystal clear because, as one of the authors of the language, to me, when it says that the Director of the CIA shall report to the Director of National Intelligence regarding the activities of the CIA, it says "shall." It does not say "may." It says "report," which to me clearly defines the relationship.

But I am gathering that some people argue that information or interpretation is ambiguous, and Mr. Powell and Mr. Smith, I want to ask the two of you about this issue. And Mr. Powell, I will start with you because I would be interested to know, in practice, when you were at the DNI, did the CIA attempt to use that language to suggest that there was ambiguity in the relationship between the Director of the CIA and the DNI?

Mr. POWELL. Senator Collins, there was discussion that there was ambiguity. I would say this: The answer to your question is, yes, there was at times discussion that somehow the statute was ambiguous.

A couple of points about that. First, I would refer you to the confirmation hearings of Director Hayden and Director Panetta where they do not suggest that there is any ambiguity in the statute in the answers to the Congress. That said, the Intelligence Reform Act was a seismic shift, and still we would hear people claim that there was ambiguity there.

I can say this. As the Chief Legal Counsel to the Director of National Intelligence, I did not see ambiguity. I spoke to the Department of Justice as to whether they saw ambiguity to it. I never had to go to the formal step of requesting a formal opinion from the Office of Legal Counsel. I did offer that option up to individuals at the Central Intelligence Agency if they continued to find ambiguity. They decided that they would rather that I did not go to the Office of Legal Counsel. I advised them as to what the oral advice was from the Department of Justice as to whether the ambiguity of the statute was there and whether they would like me to pursue it on a written basis. They said that there was no need and that we could work out the issue that we had.

So that was my experience with the statute. It is certainly consistent with what every Director of the CIA has testified about the statute. That said, there is no doubt that there are cultural and organizational issues that are going to take a decade to work out to make this community gel.

Senator COLLINS. Mr. Smith.

Mr. SMITH. Mr. Powell has said it well, but there have been instances of which I have heard, and I did not serve in government after the creation of the statute, so these are only things that one is told, that people at the CIA have pointed to the langauge and CIA supporters elsewhere around government have pointed to the language in the statute that says they report regarding activities of the CIA. That is different from the kind of language that ordinarily appears in a statute that creates a department that says the head of the department directs and controls the particular agency.

Does that language make a difference? Not really in strict legal terms, but it is enough of a difference that if an agency wishes to not adhere to the directions of the Director, there is something they can point to and give them an argument. It is unseemly, in my view, to have these kinds of arguments, but again, I think the Committee could benefit from some very frank discussions—not in public—with former Directors, both DNI and Directors of CIA, who could tell you how some of these have played out and I encourage you to do that.

Senator COLLINS. Thank you.

Mr. Nelson, just one quick final question for you, and unfortunately, I am going to have to leave. I am concerned about the difficulties that you faced in the Directorate of Strategic Operational Planning, and as I said, I readily concede that those words were a compromise. They sound contradictory. You mentioned that counterterrorism entities that do not participate face no penalty. It would help them participate, or encourage them to participate if they saw more value, and so there is a tradeoff there. But what do you think we should do with that responsibility?

Mr. NELSON. Well, with the strategic operational planning, as I suggested, I would split it into two. On the strategic part, you have to give them control over some lever. There is operations, there is the resources, there is the personnel. On the strategic level, you give them an opportunity to drive high-level policy and you give them levers over resources. And it is not only advising perhaps OMB, but it is perhaps giving them something like some sort of 1206 or 1207 type of ability to actually allocate funds in support of their operational plans. And they should be the ones writing the national strategy to combat terrorism or the national strategy against al-Qaeda. The White House should serve as the approval process and kind of massaging it, but it should come from NCTC.

And then from the operational perspective, we still in the U.S. Government lack a coordinated planning effort against terrorist groups. We have the National Implementation Plan, which you are very familiar with, that has these broad, sweeping concepts, but they are very difficult to implement in a government that executes geographically. So we look at the homegrown extremists, for example, they came from or were recruited by various entities—Lashkar-e-Taiba, al-Shabaab, al-Qaeda in the Arabian Peninsula

(AQAP). Who in the U.S. Government is saying this is the group that we need to go after first, and this is the holistic approach against it? Who is assessing that we are succeeding and what is working and what is not working? And then who is moving funds around once certain checkpoints have been reached saying, OK, now that we have neutralized this group or this threat, we need to move to the next group? That is not happening, primarily due to interagency infighting and, again, questions about authorities. Those overseas in the embassy teams will say they have the priority over there and folks back in D.C. do not.

Senator COLLINS. Thank you. That is very helpful. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. I know you have another commitment you have to go on to. I appreciate your presence here, and I am going to hold the witnesses a while longer for questioning, promising the best I can not to violate in any way the Geneva Convention. I will try not to torture you. [Laughter.]

I want to pick up with Senator Collins's questioning of you, Mr. Nelson, because the picture that you painted of NCTC's authorities and capabilities in this area of strategic operational planning is troubling, but it is very important for us to hear.

You had an interesting sentence, and I am going to look for it. NCTC "is stranded in a planning no man's land between high-level policy and strategic development and operational and tactical planning." So as I guess Senator Collins has suggested or said, we identified that there was, in fact, a no man's land as we were trying to do the legislative reform and that it was one that the government needed to inhabit in some way, that there was not sufficient connectivity between the strategic level planning and the tactical and operational planning, and that is why we created what we did.

So I wanted to ask you a couple of questions about that. You know, at that time, because we were still so close, really, to September 11, 2001, we kept coming back to this question of who is in charge of the hunt for Osama bin Laden. I know that that is not typical, and yet it is instructive in some way because we saw a lot of different activities going on, not a plan. So I want to ask you, from your experience, and you have had widespread experience at the National Security Council, the NCTC, and the Joint Special Operations Command, would you say—let us take bin Laden—who is in charge of the search?

Mr. NELSON. I think it is a great question, and again, taking it back to more theoretical and not commenting on, obviously, the operational aspects——

Chairman LIEBERMAN. Yes. Go ahead.

Mr. NELSON [continuing]. But more generally speaking, this is a problem that continues to plague the government and the counterterrorism community. There is conflict. There is no one who is actually leading these efforts or who is prioritizing these efforts.

I use the example of Osama bin Laden, we can talk about him today, but let us talk about the next al-Qaeda. What is the government entity that is going to do that? It is not being done. If it is a threat that emanates from a particular country, say for AQAP, it would be the embassy there that will say they are responsible for it. If it is happening under Title X authorities in Iraq or Af-

ghanistan, the Department of Defense would claim that they have authority.

I would just reference the Special Operations Command (SOCOM), example, where they were given authority as the supported commander in the war on terrorism. Recall how much difficulty they had in trying to get the combatant commanders, the geographic ones, to actually coordinate with them.

So this remains a significant problem. I think that until we get some sort of planning process in place that is attached to the execution and the assessment of those plans, and funds can be moved once you determine how well you are doing against a group or individual, we are going to continue to struggle——

Chairman LIEBERMAN. OK, but as I have heard you, you recommend splitting strategic from operational and having NCTC do both kinds of planning separately, is that correct?

Mr. NELSON. Well, that is right. When we tried to implement the legislation, we got beat back from the interagency on multiple occasions. Every time we trended towards the operational, there was resistance. Every time we trended towards the strategic, there was resistance from a multitude of organizations—the State Department, CIA——

Chairman LIEBERMAN. Yes.

Mr. NELSON [continuing]. Even at times, the Department of Defense, and even DHS.

Chairman LIEBERMAN. Because your statutory authority was not clear enough?

Mr. NELSON. Not clear, because what is a strategic operational plan?

Chairman LIEBERMAN. Yes.

Mr. NELSON. And because of that ambiguity, it gave them the tool to minimize or marginalize what DSOP's effect could be and impact how they actually operated. If you started doing an operational plan, they would say that is too operational, that is too tactical. You are supposed to be focused more on the strategic. If we trended towards the strategic, they would say, no, you should be focused more on the operational. So simply adding a conjunction in there clears up a multitude of issues.

Chairman LIEBERMAN. At one point, you recommend that NCTC have some authority to control and allocate funds to the departments. Is that one way to establish its primacy here?

Mr. NELSON. Well, we do. We have to give them some sort of lever to compel the interagency to participate, and if we are not going to give them operational authority, then we need—to look at resources and personnel. Giving them some input, a direct input over resources, hopefully would encourage interagency participation in these plans.

Chairman LIEBERMAN. Let me give you an example which is obviously not so far from reality, leaving aside bin Laden. But let us say that in Somalia, there is an American who has become a radical Islamist cleric. He runs Web sites which are in English and he is communicating a lot with people in America and people in America are communicating with him. He is helping to radicalize them. Sometimes, he brings them over. They come to see him. He has be-

come dangerous to the United States and, in fact, has been implicated in some terrorist attacks on our country.

So let us just sort of clear the deck of what exists now. It would certainly seem to me that it would be in the interest of our government to have a plan to capture or kill that person, and so how would you organize that if you were redrawing the structure now?

Mr. NELSON. I think NCTC has the authority to do this under the current structure. I just think that they are having a difficult time getting agencies to participate.

Chairman LIEBERMAN. Right, because, obviously, NCTC does not have the resources itself to carry out an operation.

Mr. NELSON. Absolutely. They have no authority.

Chairman LIEBERMAN. Yes.

Mr. NELSON. And as I said, planning is everything, but those planners have to be the ones that are executing. In NCTC, a role I think, that is underutilized, is that of arbiter. We have discussions on many issues for example, the Web site issue—do you take the Web sites down? Do you keep the Web sites up? How does that work? Some of those decisions go to the very highest levels of government, and as my colleagues mentioned, some should not. Somebody should be arbitrating those decisions at a much lower level and that is a role that NCTC could undertake, but it cannot do because it does not have the credibility and the authority currently to do that.

Chairman LIEBERMAN. Let me ask Mr. Smith and Mr. Powell if you have an opinion on this question. There is a problem, which is how do we coordinate the various branches of our government in planning and carrying out coordinated operations.

Mr. SMITH. Mr. Chairman, that is one of the reasons I am attracted to the Goldwater-Nichols model.

Chairman LIEBERMAN. Yes.

Mr. SMITH. In Goldwater-Nichols, a combatant command is given the responsibility for a geographic area to go do something, to carry out a mission. The only one that does not have that is SOCOM, which has a global mission. And by the way, we just saw in Afghanistan General Stanley McChrystal decide that he needed greater authority over forces under SOCOM for the very reasons that we are talking about——

Chairman LIEBERMAN. Right.

Mr. SMITH [continuing]. One of the first things you learn in military life is unity of command and that has to be, and it seems to me it has to be here, as well.

I am not remotely able to talk with the kind of expertise that Mr. Nelson has spoken with respect to planning. However, instinctively, I would think that a mission such as the one you described should be given to an operating entity and that operating entity should have the responsibility to develop the plan and then run it by NCTC, much as a combatant command consults with the Joint Staff about any plans they develop.

Chairman LIEBERMAN. So how do we do that in this case? Let us take the radical cleric that I described, and I put him in Somalia for the sake of it being hypothetical. Who would be the combatant commander in that case?

Mr. SMITH. I think, in my view, it should be Africa Command (AFRICOM).

Chairman LIEBERMAN. AFRICOM? Fascinating. So to go to the military command and then have that person coordinate with all the resources—intelligence, State Department, all the rest?

Mr. SMITH. That is correct, because I think at the moment, the Defense Department has the greatest reach, the greatest capacity.

Chairman LIEBERMAN. Right.

Mr. SMITH. But they cannot over-militarize it, if I could use that expression.

Chairman LIEBERMAN. Yes.

Mr. SMITH. And that is where the role of the NCTC has to come in, much as the role of the Joint Staff has to come in, to say, your plan does not take adequate account of this or that and that then has to represent other—and the advantage of NCTC stepping in is they represent—and there are representatives on there—of other departments and agencies of government that would bring a perspective to it, that would bring information to it to refine that plan, but that it would ultimately have to be executed by AFRICOM.

Chairman LIEBERMAN. Mr. Powell, that was very interesting. Your reaction?

Mr. POWELL. I think that on the specific operational tasking and coordination of them, there are operational deconfliction agreements in place between agencies that I think work fairly well in the field. It may just reflect the lack of knowledge on my part, but I did not see in the field—I saw the agencies working together. The closer you are to the mission, the more some of these debates go away.

I would be very concerned and want to think heavily about bringing a tactical operational type of planning function away from those agreements that I, frankly, think in my experience have worked well in specific operational tasks of the kind of hypothetical that you are talking about, Mr. Chairman. I think the NCTC has a lot of value to add on the broader issue of not just an operation about a specific person or more at the tactical level, but more what are we doing as a government to counter the fact that there are people here in America who are going to visit this cleric in your hypothetical——

Chairman LIEBERMAN. Right.

Mr. POWELL [continuing]. And becoming radicalized or becoming self-radicalized or accessing Web sites. And, of course, these are by far what we have seen recently some of the most dangerous threats and the most hardest to detect are people self-radicalized, not necessarily connected to al-Qaeda, AQAP, or some of the other organizations we can talk about, and obviously the attention that those organizations draw from the U.S. Government. But there is a large value in thinking about at the level that NCTC can about what do we do about that phenomena and problem. Obviously, there has been talk about problems in prisons. Here in the United States, we can talk about any number of these things.

I think at the tactical hunt level, and obviously Mr. Nelson has far more experience in this than I do, but just going back to my military experience and other ways, and I certainly was very concerned from the Director of National Intelligence standpoint, any

time that we seemed to veer into tactical operational issues or had to become involved with them, I did not think that we had the rules, the guidelines, the capabilities present to get involved. Now, some major national issues at times may draw in some of the senior staff, but that was very unusual and rare.

Chairman LIEBERMAN. That is a very helpful answer.

Let me ask you just one or two more questions. I will start, Mr. Smith, in your prepared statement, you discussed complaints by officials in various agencies that the DNI staff often acts as micromanagers and issues time-consuming requests and data calls to agencies for information for reasons that are often not very well understood. You also note that this information request process quite often appears to be driven by contractors at the DNI.

Well, first I will ask you, Mr. Smith, because you say that from your perspective, the current Director, Admiral Blair, is not interested in micromanaging intelligence agencies. I wonder if you would speak a little about that and whether you know whether he has taken steps to address the issue you raise of what you might call over-tasking.

Mr. SMITH. The answer is, I believe, yes to all your questions, Mr. Chairman.

Chairman LIEBERMAN. [Laughter.]

Mr. SMITH. Director Blair does not intend to micromanage. He understands he cannot do that. On the other hand, he has a great many responsibilities under the statute and he has inherited a structure where there are already a lot of contractors in place. I cannot begin to speak for him, but he is aware of this issue. There are ways that one could try to get a handle on the tasking that ODNI does so that it is coordinated and that only tasks are issued are those that senior leadership truly believes are necessary. I cannot speak, because I simply do not know what the Director might be doing to address that issue, but I do know he knows it is an issue.

Chairman LIEBERMAN. Mr. Powell, was this a problem, to the best of your recollection, when you were at the ODNI?

Mr. POWELL. It was continually at the front of issues that were raised with former Director Negroponte, former Director McConnell, and now——

Chairman LIEBERMAN. Yes.

Mr. POWELL [continuing]. Director Blair. It was an issue of continual discussion every week, about the issue of tasking, about the complaints we would read in the newspapers about this, about issues we would hear in the Congress about these issues.

My first response to those would often be, please give me the specific example that you are speaking about.

Chairman LIEBERMAN. Right.

Mr. POWELL. I often had a very difficult time of finding what the specific example was.

Second, the issue was, if the DNI's Office sends out something that is inappropriate, well, you should call the Deputy Director of National Intelligence, one of them, and tell them that something inappropriate is going on and it needs to be put to a stop——

Chairman LIEBERMAN. I am sorry. Do you think it was real, or do you think this was just bristling by the agencies that were getting used to dealing with the new Office of the ODNI?

Mr. POWELL. There is no doubt that there were, I am sure, requests that were sent out that I did not think were appropriate to be sent out.

Chairman LIEBERMAN. Right.

Mr. POWELL. That said, for the first time, we did a contractor inventory of the entire intelligence community and could tell you the functions of what these contractors are doing.

Chairman LIEBERMAN. Yes.

Mr. POWELL. The Congress found that very interesting.

Chairman LIEBERMAN. Yes.

Mr. POWELL. The intelligence community found that very interesting from a budget perspective.

Chairman LIEBERMAN. Too many?

Mr. POWELL. I will just say that we did the contractor inventory, Chairman Lieberman, by the function, and I do not want to make any broad generalizations about it, but it gave you an idea and you could then look to see by function what are people doing in the community, and that gave you data points then to make budget decisions. That, in my experience, is the very first time you got a picture of what the workforce looked like, who speaks what languages across the intelligence community.

So all these things did require data calls. The law on joint duty is a perfect example. There are a number of things in there by law about promotion rates, that people who participate in joint duty cannot be promoted at a rate lesser than their peers who do not participate in joint duty.

So it is a fine balance. I am sure that there are examples where the DNI's Office overtasked or did something that they should not have. There were rules put in place. At one point, I think any data request of this type had to go through a three-star general on the DNI staff to do this. So this was not something that did not have the Director's attention.

Chairman LIEBERMAN. Right.

Mr. POWELL. I think if you look at the Secretary of Defense's Office, the Secretary of State's Office, or the Attorney General's Office, I suspect at times perhaps they send out tasking requests that are not needed.

Chairman LIEBERMAN. I am sure that is right.

Let me ask you a final question. When Governor Kean and Congressman Hamilton testified before us in late January, they raised the idea, kind of floated it, of whether the DNI should have a fixed term of service similar to that of the FBI Director on the theory that would improve continuity and to a certain extent remove the DNI, to whatever extent he is involved in the political process now, from that process, or at least from the transition of government. I am interested in just getting a quick reaction from the three of you. Mr. Smith.

Mr. SMITH. It is a good idea, very worthy of consideration. I think it has worked at the Director of the FBI and I think it is a good idea. Some of the downsides, however, are it is hard to find somebody willing to commit to an extended period.

Chairman LIEBERMAN. Right.

Mr. SMITH. You want somebody who is close to the President, who can pick up the phone and say, Mr. President, you have a problem here, and not be intimidated because he or she does not have a relationship with the President.

So it is a serious question that should be examined. If I were to vote today, I am a little like the Supreme Court. I am five-to-four against it——

Chairman LIEBERMAN. OK.

Mr. SMITH [continuing]. But I could be persuaded.

Chairman LIEBERMAN. Mr. Nelson, how does your Supreme Court rule?

Mr. NELSON. I actually think it is a very intriguing decision. I would be in support of it. To finish the kind of change that you put forward in the legislation, the IRTPA, it is going to require some china to be broken and that individual needs some political topcover to make that happen. I was very disturbed and disappointed in the decision that was made regarding the appointment authority of the DNI representive overseas. I think that was the wrong call. I think maybe something like this would have been able to address that.

Chairman LIEBERMAN. Mr. Powell.

Mr. POWELL. I am probably seven-to-two or eight-to-one against it. [Laughter.]

I should note, I clerked for a Justice who was often on that one side, so——

Chairman LIEBERMAN. The only time I got to argue a case before the Supreme Court when I was Attorney General of Connecticut, we lost eight-to-one, so I am sympathetic to that Justice. [Laughter.]

Mr. POWELL. I think the Director of the FBI is a very special case. There is a history there. I worked at the FBI. There is a history behind that. The FBI Director has access to information on the law enforcement side in terms of investigating senior officials of the government and other things that are very distinct from the DNI.

My concerns would be: One, you do have a statute that does require the President's backing. I would be very concerned if you had, for whatever reason, a place where the DNI was kept out of the national security circle——

Chairman LIEBERMAN. Yes.

Mr. POWELL [continuing]. And seen as really apart from it. I think the information is so critical, the operational issues, the issues we are dealing with on intelligence, whether it is Iran, North Korea, Afghanistan, Iraq, cyber threats coming over the horizon, issues in Africa, all those things.

I worry about having a lengthy term could really impact that and have a problem. I think it would raise the bar to the extent that you had somebody who was not performing up to perhaps the full capabilities that they needed to be. It would be a very difficult thing to remove them. It would then be seen as a very political move. There would be all kinds of allegations.

Chairman LIEBERMAN. Right.

Mr. POWELL. So I would be very concerned about any type of lengthy term for a DNI. In my experience, having served the three

Directors of National Intelligence, I just have not seen this evidence of politicization or changing the intelligence or trying to rework it. I think, frankly, given the diversity of who produces that intelligence, that is a very difficult thing to do with the National Intelligence Board and the other analysts who are involved in the process.

Chairman LIEBERMAN. Thank you. Thoughtful responses. Thanks very much for your testimony. This has been very helpful.

Do you want to add something?

Mr. SMITH. Just as a matter of personal privilege, Mr. Chairman——

Chairman LIEBERMAN. Yes, please.

Mr. SMITH. At the outset of his remarks, Mr. Powell said some extraordinarily kind things about me.

Chairman LIEBERMAN. Yes.

Mr. SMITH. I am not sure they were justified——

Chairman LIEBERMAN. Do you want to deny them? [Laughter.]

Mr. SMITH. I would like to correct them for the record, but I do appreciate them greatly, especially coming from Mr. Powell, who has had himself an extraordinary career of contributions to this country.

Chairman LIEBERMAN. Well, that is nice of you to say, very gracious. Really, it could be said of all three of you. We appreciate it very much.

You have been very helpful today. Senator Collins and I are quite serious about this review, and we are not intent on legislating unless there is a reason to legislate, but if there is, we are not going to hesitate if we think it can improve and strengthen what was begun with the 2004 Intelligence Reform and Terrorism Prevention Act.

I appreciate also that the three of you did some work in preparing for this testimony today, which matters a lot to us, and obviously the full text of your statements will be entered into the record. But Senator Collins and I and our staffs really would like to continue to be in touch with you as we go forward with this oversight. We are now going to talk to some of the people who are at the agencies now and probably best start that in closed sessions so that we can get maximum information.

I am going to leave the record of this hearing open for an additional 15 days for any statements or questions that others may have.

And with that, I thank you for your continuing service to our country. The hearing is adjourned.

[Whereupon, at 12:20 p.m., the Committee was adjourned.]

THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: SECURING THE VISA PROCESS

WEDNESDAY, APRIL 21, 2010

U.S. 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, Carper, Collins, McCain, and Voinovich.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. I apologize for keeping everyone waiting for a moment or two.

This is the fifth in a series of hearings our Committee has held to examine our intelligence and security systems that, despite all we have done to strengthen them, allowed Umar Farouk Abdulmutallab to board a U.S.-bound airliner and attempt to blow it out of the sky over Detroit last Christmas Day.

I want to welcome our witnesses here today, each of whom has a critical role to play in helping ensure that this type of failure does not happen again, and I would also say each of whom has become quite familiar to our Committee.

The purpose of this hearing is to review the enhancements to our visa security system that have been made over the last few years, the last 5 years particularly, but specifically to get a progress report on enhancements that have been put in place post-Christmas Day, including changes to how the State Department processes and disseminates information it receives about terrorism in its consulates abroad and also to have a good discussion about what additional changes may be needed.

The failures that allowed Abdulmutallab to board Northwest Flight 253 are by now familiar to us all: Warnings from the father which went unheeded, threats from Yemen which were not run to ground, and information in different databases that was still not connected.

However, one of the most frustrating failures was one that would seem to have been easiest to avoid, which is the misspelling of Abdulmutallab's name during a check of the State Department's

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00161 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

visa database, which led the government to believe that he did not have a visa and so did not pose an immediate threat.

I think we all need to understand that while America has been and remains probably an open country that welcomes visitors, international travel is a privilege in our time and not an absolute, unlimited right.

My concerns about the security of the visa process were one of the reasons that we advocated giving the Department of Homeland Security (DHS) more authority over the visa-issuing process during the debate and legislative action during which we actually created the DHS. The events of Christmas Day, I must say, have brought me back to some of those ideas.

Nine years after September 11, 2001, we still do not have an automated system in place to check for revoked visas as individuals board airplanes. I understand that the State Department and DHS are working to accomplish this in an expeditious manner, and I hope to hear reports on that today.

When the Department of Homeland Security was created, as another example of the overlap of the two Departments and what we can do to deepen it and expedite it, Congress included a provision establishing the Visa Security Program (VSP) and giving DHS the authority to set visa policy and to deploy law enforcement officers to consulates in order to oversee the visa-issuing process because of the post-September 11, 2001, added security dimension.

The idea was to ensure that security considerations were given the weight they deserve in visa issuance. Eight years later, I am sorry to come to the conclusion that the program has not been a priority for either Department, and I would like the witnesses to comment on that.

Here is why I reach that conclusion. DHS and the State Department have identified 57 high-risk consular posts around the world. That is out of a total of more than 200 posts that issue visas. But only 14 of those ports have received, or had stood up in them, Visa Security Program Offices.

The President's fiscal year 2011 budget submission does not include any new money for continuing to expand this vital program.

I understand that one of the main impediments to expanding the program, aside from funding, has been reluctance by some of our Ambassadors to allow the Visa Security Program Offices to be established at their posts, and I would like to hear about that if that is true.

I gather that on at least seven separate occasions, ambassadors have told the Department of Homeland Security that they would not support expansion of the VSP at their embassy. And some of those posts are ones that are really key in fighting against terror, such as the United Kingdom, Turkey, and Indonesia. It was not our intention when we put this provision into the Homeland Security Act to give Ambassadors veto power over this important program.

So I look forward to hearing from the witnesses and to working with DHS, the Department of State, and our colleagues on Foreign Relations to ensure that the VSP program does move forward.

Finally, I am heartened that for travelers from visa waiver countries, the Department of Homeland Security has now fully implemented the Electronic System for Travel Authorization (ESTA),

and is making progress in signing the international information-sharing agreements that are required by law. That is a significant accomplishment.

The Christmas Day attempted attack has underlined for us all the importance of effectively sharing information. I believe that expanding this information sharing to include our allies should be one of the Department of Homeland Security's main priorities moving forward, and so I hope the State Department will expedite implementation of the agreements to ensure that information is being shared in real time.

Securing our homeland is now really a global enterprise. It begins well before people come to the United States, and that is why it is so important that the Departments of State and Homeland Security are working closely and effectively together.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Today's hearing will examine the fundamental question of why the Christmas Day bomber, Abdulmutallab, was allowed to retain his visa, even after his father had informed the American embassy in Nigeria of his Islamist extremist connections.

From my perspective, the State Department had sufficient information to revoke Abdulmutallab's visa. State Department officials already had decided to question him about his ties to extremists if he chose to renew his visa. That he could have been deemed a threat to the United States in the future based on his extremist ties but not a sufficient current threat defies both logic and common sense. Had the State Department taken this action, it would have prevented him from traveling to the United States. This was a missed opportunity to stop the terrorist more than a month before his flight.

At the very least, Abdulmutallab should have been required to come to an American embassy and explain his activities before he was allowed to travel to our country. The State Department has this authority, and, in fact, the Intelligence Reform Act protects the State Department from lawsuits when its officials revoke a visa for a visa holder overseas. But the State Department failed to act.

Visa holders with possible connections to terrorism should shoulder the burden of proving that they do not intend to harm this Nation or its citizens. I agree with the Chairman's statement that traveling to our country is a privilege. If they cannot meet that burden, then we cannot take the risk of permitting them the privilege of traveling to our country.

Following the attempted attack on Christmas Day, the intelligence community has reviewed the visas of all persons listed in the broadest terrorist database, known as the Terrorist Identities Datamart Environment (TIDE), to determine whether or not they should be permitted to retain their visas. In my judgment, they should keep their visas only in exceptional circumstances that are carefully considered by the State Department, intelligence community, the Department of Justice, and the Department of Homeland Security.

There are essential policy issues that we will explore today. First, is there now an ongoing policy to check the TIDE list for individuals who hold U.S. visas? Second, what is the Administration's current policy on the revocation of the visas held by individuals listed on the Terrorist Identities Datamart Environment TIDE list? Third, what is the policy on visa revocation for individuals that are on the terrorist watchlist?

I was surprised to learn recently from the Government Accountability Office (GAO) that more than 1,000 individuals on the narrower terrorist watchlist had U.S. visas.

Revoking the visas of suspected terrorists is, however, only the first step. The Department of Homeland Security also should confirm the validity of the visa of every foreign passenger who attempts to board an airplane to this country rather than waiting until his arrival in our country. There does not appear to be a technological barrier since DHS already confirms whether a passenger is on the No Fly or the Selectee List before the passenger boards the plane.

Like the Chairman, I also want to know how the State Department will ensure that minor misspellings do not prevent its officers from discovering immediately that a suspected terrorist has a valid visa, as initially happened with Abdulmutallab. Computer algorithms have been around for a long time that can find close name matches to uncover a misspelling, and the State Department should expeditiously adopt such tools.

In general, I believe that the Department of Homeland Security must provide greater oversight of visa issuance and revocation, as it was authorized to do in the Homeland Security Act of 2002. That Act requires DHS to deploy trained visa security officers to overseas posts, but DHS has only reached 14 of the 57 high-priority foreign posts—with plans to reach another four. Why has the joint effort of DHS and the State Department to expand this program been so slow?

One important way that DHS is enhancing the security of the visa process is through the implementation of a requirement that Visa Waiver Program travelers receive an electronic travel authorization, as the Chairman mentioned in his opening remarks. This additional step should add an important security layer for travelers from countries that are currently not required to obtain a visa.

It is clear that terrorists will continue to seek to exploit any vulnerabilities in our visa system. We must, therefore, continue to work to strengthen our visa process. Since this is the primary means of preventing terrorists from traveling to our country, it must work effectively, and it must be a priority.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much, Senator Collins.

Let us begin the testimony, Mr. Heyman, with you, I think by consent of the witnesses. David Heyman is the Assistant Secretary of Homeland Security for Policy. Please proceed.

TESTIMONY OF HON. DAVID F. HEYMAN,[1] ASSISTANT SECRETARY, OFFICE OF POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HEYMAN. Thank you, Chairman Lieberman, Senator Collins, Senator Voinovich, and other Members of the Committee. I appreciate the opportunity to appear before the Committee.

The work in the area of promoting and overseeing secure travel to the United States is very important, and specifically securing the visa process and related lessons and implications of the Christmas Day attack, which is the focus of this hearing.

Targeting terrorist travel is one of the most powerful weapons we have to counter the ability of terrorists to operate. Travel security involves a series of tools or layers to help identify and disrupt terrorist travel. It begins with international travelers obtaining legitimate identity documents from national authorities—a passport—and should a visa be needed, the international traveler then applies for one at a U.S. embassy or consulate and undergoes a personal interview and checks against law enforcement, terrorism, and immigration databases. Travel security also includes passenger and baggage screening prior to travel and during travel flight security through air marshals. We have also put in place hardened cockpit doors and other measures. Finally, it includes passport control and customs and immigration inspection upon arrival—or in some locations, prior to departure. Every step along this pathway presents a vulnerability to would-be attackers who must come out of the shadows and interact with security personnel at ports of entry and abroad.

In terms of visas and visa security, foreign travelers to the United States come to the attention of U.S. officials either by applying for a visa at a U.S. embassy or consulate or by traveling to the United States under a visa-free program, one of which, the Visa Waiver Program, requires advance authorization, as the Senator has noted.

The Department of State is responsible for the day-to-day operations of visa issuance. DHS' role in visa policy and guidance is outlined in Section 428 of the Homeland Security Act, which gives the Secretary the authority to issue regulations with respect to the granting of or refusing visas.

As demonstrated by the attempted attack by Umar Farouk Abdulmutallab on December 25, 2009, visa policy and proactive visa screening procedures must be addressed in a counterterrorism context. To that end, they must include functionally related measures such as document verification and enhanced international information sharing. Taken as a whole, these procedures help to ensure not only the integrity of our borders and our immigration system, but also the security of the traveling public and the global aviation system as well.

The first part of travel security is the authorization step, which is the focus of this hearing. My colleague, John Morton, from Immigration and Customs Enforcement, will testify on DHS' Visa Security Program. Ambassador Janice Jacobs, Assistant Secretary for Consular Affairs, will discuss the visa issuance process. For my

[1] The prepared statement of Mr. Heyman appears in the Appendix on page 458.

part, I will limit my testimony to the Visa Waiver Program (VWP), which was first authorized by Congress as a pilot in 1986. The purpose was to facilitate low-risk travel to the United States and boost international trade, cultural links, and promote more efficient use of consular resources. It has evolved into an important tool for increasing security standards, advancing information sharing, strengthening international partnerships, and promoting legitimate trade and travel to the United States.

Since the program's inception, Congress and the Executive Branch have worked together to implement a number of security enhancements, including, immediately after September 11, 2001, new requirements to tighten security of passport standards and increase the frequency in which visa waiver countries are formally reviewed for their designation status.

Today VWP allows citizens from 36 countries to travel to the United States without a visa and, if admitted, to remain in the United States for a period of a maximum of 90 days for tourist or business purposes.

There are a number of security benefits that the Visa Waiver Program produces. They are, in fact, mutually reinforcing. VWP requires bilateral information-sharing arrangements regarding known or suspected terrorists, possible perpetrators, and other serious crimes, as well as multi-lateral sharing of lost and stolen passport information. Moreover, there are higher standards for transportation security, aviation security, and border security as well as document integrity than for countries that do not participate in the program. DHS, with the support of the Departments of State, Justice, and the intelligence community, audits these standards and capabilities on a regular basis as a condition for continuing designation in the program. No other mechanism provides DHS with the opportunity to regularly conduct as broad and consequential inspections of foreign security standards as the VWP.

We are also strengthening that program currently by entering into agreements to share information that the Chairman mentioned. This is particular important in the context of the failed terrorist attempt to bring down Northwest Flight 253. We must absolutely bolster the tools we have to screen passengers prior to departure and exchanging information regarding potential threats known to our partner countries but perhaps not to us as a vital element of that.

We have three key mechanisms that support this effort: First, a bilateral arrangement to exchange information on known and suspected terrorists; second, a bilateral agreement to exchange information of possible perpetrators of serious crimes; and, third, an exchange of diplomatic notes memorializing the commitment to report lost and stolen passports according to Interpol standards.

As Senator Lieberman mentioned, our current priority and primary focus of DHS, as it relates to Visa Waiver, is bringing the 27 pre-2008 VWP countries into compliance with the 9/11 Commission Act information-sharing requirements by 2012. To date, the Department, in cooperation with its partner agencies, has made substantial progress in this endeavor, the details of which are included in my full testimony.

Let me conclude by looking into the future. Given the security benefits of the VWP to the United States and to the program's important role in strengthening international partnerships and to travel security standards, the Department would support a carefully managed expansion of the VWP to select countries willing and able to enter into a close security relationship with the U.S. Government, particularly DHS.

At present, most of the countries that have expressed an interest in VWP designation have visa refusal rates higher than 3 percent or they have other concerns that would have to be mitigated prior to designation. DHS and the Department of State continue to consult with trusted international partners to determine whether VWP designation is possible in the future. We are also pursuing, as resources allow, VWP-style information-sharing agreements with countries that are currently ineligible for the VWP but have reasonable expectations of qualifying for the program within the next 5 years or so.

We must also be able to review and account for overstays. Because DHS has not yet notified Congress that a biometric air exit system to help in this is in place, any significant expansion of the VWP is unlikely at the present.

So, in summary, we know that no single entity and no single solution on its own will completely address the challenge of preventing those with bad intentions from traveling to the United States. Travel security systems of mutually reinforcing layers—involving such features as rigorous visa issuance standards, the use of visa security units, the screening of passengers through automated targeting systems, and forward-deployed border and immigration security officers—all of these are critical in our efforts to thwart the travel of terrorists and other dangerous people. The VWP is, of course, a vital part of a robust travel security system for many reasons: The ESTA requirement, as Senator Collins mentions; the mandatory bilateral information-sharing arrangements regarding potential terrorists and criminals; sharing of data for lost and stolen passports; inspections; security standards; and the monitoring of ongoing conditions in countries. It is one of a number of tools and layers we deploy to protect the United States at home, in the air, and abroad.

Chairman Lieberman, Senator Collins, and other distinguished Members, thank you for the opportunity to appear before you today. I look forward to your questions.

Chairman LIEBERMAN. Thank you, Mr. Heyman, for your statement. We will go next to Hon. Janice Jacobs, Assistant Secretary of State for Consular Affairs. Welcome back.

TESTIMONY OF HON. JANICE L. JACOBS,[1] ASSISTANT SECRETARY, BUREAU OF CONSULAR AFFAIRS, U.S. DEPARTMENT OF STATE

Ms. JACOBS. Thank you. Chairman Lieberman, Ranking Member Collins, Senator Voinovich, and distinguished Members of the Committee, it is an honor to appear before you again and to explain the

[1] The prepared statement of Ms. Jacobs appears in the Appendix on page 465.

Bureau of Consular Affairs' efforts to strengthen the security of U.S. borders through the vigilant adjudication of visas.

I want to assure you that the five pillars of visa security—technological advances, biometric innovations, personal interviews, data sharing, and training—about which I testified previously—are still very relevant today. And each pillar to an appropriate extent informs every action we have taken following the attempted terrorist attack of Christmas Day 2009.

Over the past 4 months, we have strengthened our Visas Viper reporting requirements, as well as visa issuance and revocation criteria, and introduced technological and procedural enhancements to facilitate and strengthen visa-related business processes. Our internal and interagency reviews are ongoing. Here are the steps that we have taken already.

The Department of State misspelled Umar Farouk Abdulmutallab's name in a database search for existing visas and in the text of a Visas Viper report. As a result, we did not add the information about his current U.S. visa in that report.

To prevent this from occurring again, we promulgated new Visas Viper procedures to ensure that in preparing a Visas Viper report we ascertain whether a subject has a visa and include comprehensive visa information in all Visas Viper reporting. I can confirm that these new procedures have been followed in all Visas Viper cables since December.

We also are re-evaluating the procedures and criteria used in the field to refuse and revoke visas, and we are issuing new instructions to our officers. Revocation recommendations will be added as an element of reporting through the Visas Viper channel. In a recent cable to the field, we reiterated our guidance on use of the broad discretionary authority visa officers have to deny visas under Section 214(b) of the Immigration and Nationality Act with specific reference to cases that raise security or other concerns. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

The State Department has broad and flexible authority to revoke visas. Since 2001, we have revoked 57,000 visas for a variety of reasons, including over 2,800 for suspected links to terrorism. New watchlisting information is continuously checked against the database of previously issued visas. We can and do revoke visas in circumstances where an immediate threat is recognized. We can and do revoke visas at the point people are seeking to board an aircraft, preventing their boarding. In coordination with the National Targeting Center, we revoke visas under these circumstances almost daily.

At the same time, the benefit of expeditious coordination with our national security partners is not to be underestimated. There have been numerous cases where our unilateral and uncoordinated revocation would have disrupted important investigations that were underway by one of our national security partners. We will continue to closely coordinate visa revocation processes while also constantly making enhancements to the security and integrity of the visa process. Information sharing and coordination action are foundations of the border security systems put in place since September 11, 2001, and they remain sound principles.

Had our post-December 25 Visas Viper and revocation procedures been in place in Abuja, Nigeria, in November 2009, the consular officer would have used our robust search engine to uncover Abdulmutallab's visa record and include that name in the Visas Viper cable. The consular officer would have entered a P3B—a possible terrorist—entry into the Consular Lookout and Support System (CLASS), our automated repository of watchlist information—as was done in the actual case.

The Department would have reviewed the Visas Viper cable upon receipt and, following expedited consultation with our interagency partners, revoked Mr. Abdulmutallab's visa, consistent with our post-December 25 policy that no one with a P3B entry can hold a valid visa. This revocation would have occurred on the day the Visas Viper cable was transmitted.

The Department has close and productive relationships with our interagency partners, especially with the Department of Homeland Security. We are working closely with Immigration and Customs Enforcement visa security units (VSUs). VSUs currently operate at 14 visa-adjudicating posts in 12 countries. Since January of this year, we have received requests to open four additional VSUs and to augment staff at two existing VSUs. The chiefs of mission at those respective posts approved the four new VSUs and one request for expansion, with one request for expansion still pending. Later this year, a team representing both departments will visit several posts under consideration for additional VSUs.

The State Department brings our own unique assets and capabilities to this partnership. Our global presence, international expertise, and highly trained personnel provide us singular advantages in supporting the visa function throughout the world. We developed and implemented an intensive screening process requiring personal interviews and supported by a sophisticated global information network. Our front line of border security has visa offices in virtually every country of the world, and they are staffed by highly trained, multi-lingual, culturally aware personnel of the Department of State. We support them with the latest technology and access to advanced screening tools and information systems. We are pioneers in the use of biometrics and a leader in the use of facial recognition as well as modern rapid fingerprint scanning technology.

Our online visa applications, introduced in 2009 and on track for worldwide deployment before the end of this fiscal year, expand our data collection capacity tenfold and provide new information readily available for analysis by the State Department and other agencies.

We remain fully committed to correcting mistakes and any deficiencies that inhibit the full and timely sharing of information. We fully recognize that we were not perfect in our reporting in connection with this case. However, we are working and will continue to work not only to address shortcomings but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

We 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 exchange of ideas. In fact, the United States must strive to meet both goals to guarantee our long-term security.

Thank you, and I am ready to answer your questions.

Chairman LIEBERMAN. Thanks, Secretary Jacobs. I think Senator Collins and I would like to break the normal and just ask you a few questions to make sure that we have clear the changes that the Department has made.

First, just set out kind of what we used to call a plain-language definition of what Visas Viper cable is.

Ms. JACOBS. A Visas Viper cable is a reporting telegram that comes in from our posts overseas, reporting on names of known or suspected terrorists. The process behind it includes a Visas Viper group, interagency group, at an embassy or consulate overseas that sits down at least once a month to go through to see whether each of the agencies involved might have names that need to be submitted to Washington. These names will result in the creation of a TIDE file by NCTC.

So it really is, if you will, an interagency data-sharing program at the post level where they are bringing names back to Washington.

Chairman LIEBERMAN. OK, good. That is helpful.

Now, in Abdulmutallab's case, as we know, when the State Department personnel in Nigeria put his name into the database, it did not show he had a visa because his name was misspelled. Correct?

Ms. JACOBS. That is correct.

Chairman LIEBERMAN. And so what I think we are both interested in is—it is our understanding that there is a software program that can correct for those misspellings. Do I understand that has now been put into place in the State Department?

Ms. JACOBS. Yes, sir. We actually had a search tool that uses what we call "fuzzy logic" that will catch misspelled names. It was not available to all of our consular officers in the field. The change that we have made now is that we are requiring all officers, whenever they are drafting a Visas Viper telegram, to use that search tool in order to look in the database of issued visas to make sure that a misspelled name will not make a difference.

Senator COLLINS. Just to clarify the Chairman's question, that technology was already in place, but it was not automatically used?

Ms. JACOBS. It was not used for searches in the Consolidated Consuler Database (CCD) where we store all of the information about visas. We have very sophisticated search capabilities in our Lookout System, but that same tool was not used on a routine basis in our CCD. So it was there. It was used primarily by our fraud prevention officers, but now we have made it a requirement that everyone use that tool.

Senator COLLINS. It seems to me you would want to just build it into the system so that it is not a choice. It is the way, when we go online with Google and if you misspell something, it says, "Did you mean X?" and will give you the proper spelling of it. Should that be automatically built in?

Ms. JACOBS. Absolutely, and we are working on that systems change to make that automatic within the CCD.

Senator COLLINS. And when do you anticipate that will be an automatic feature of the search?

Ms. JACOBS. I will get back to you with an exact date. I am hoping that will happen within the next few months. But in the meantime, all officers have been instructed to use this tool whenever they are preparing Visas Viper cable.

Senator COLLINS. I understand that, but I guess what I am troubled by is it is still discretionary in a way. Even though they have been instructed, it is not built into the system, and it seems as if it would be very easy from a technological standpoint to build it into the system. So rather than chancing that some consular officer who is overwhelmed with work might forget to use it or might fail to use it, why not build it into the system?

Ms. JACOBS. We will do that, and I will get back to you with a date certain when we will have that completed.

Senator COLLINS. Thank you for letting us clarify that.

INFORMATION SUBMITTED FOR THE RECORD

When visa applications are entered into consular databases, names are automatically run through "fuzzy logic" algorithms that check against the Consolidated Consular Database (CCD) and the Consular Lookout and Support System (CLASS). When names are added to the CLASS database independent of visa applications, officers are instructed to check the name against the CCD for possible matches with visa records using the "Person-Finder" tool, which uses the same "fuzzy logic." This is currently a manual process, but we will have the automation in place by July 31, 2010.

Chairman LIEBERMAN. Thanks. Let me go the next step. Let us assume now that we have the system and it checks for the spelling, and a Visas Viper cable is sent back on an individual with the suggestion or evidence that he or she may be associated with terrorism. And the next step, as you described it in your testimony, I was concerned you had some conditional words. Will that automatically lead at least to the suspension of the visa, if not the revocation, but at least to the suspension? In other words, it does not require any more than that Visas Viper cable that person now does not have an effective visa anymore?

Ms. JACOBS. Right. In this particular case, the new search tool would have caught the misspelled name. In addition, officers are required now to put the fact that a person has a visa right in the Visas Viper cable, so that information would be there. And then the fact that the officer put an entry, a "presumed ineligible for terrorist-related reasons" entry, into our Lookout database, that information would have been in the Visas Viper cable as well.

Our new policy is anyone who goes in as a P3B who has a visa, the visa will be revoked. We do that still in consultation with our other agency partners to make sure that there is no operational interest in the individual. That happens very quickly now——

Chairman LIEBERMAN. An "operational interest" in the sense that we actually may want the person to have the visa because we are following him or her.

Ms. JACOBS. Exactly right.

Chairman LIEBERMAN. OK. Understood.

Ms. JACOBS. And, anyways, that would happen very quickly. We have expedited the whole revocation process while we still have the system where names go into NCTC and are reviewed and then cer-

tain names are exported over to the Terrorist Screening Center. In addition to that, we have a new expedited procedure in place whereby consular officers can make a recommendation about a revocation, or if they put someone in as a P3B, we will revoke after consultation.

Chairman LIEBERMAN. OK. Am I right that also is a change since Christmas Day?

Ms. JACOBS. Yes, sir.

Chairman LIEBERMAN. That it was not automatic that the visa be revoked?

Ms. JACOBS. Right. No, before Christmas Day it was not.

Chairman LIEBERMAN. OK. Those are two big steps forward, and I appreciate them.

Let me just poke a little more into the operations. I was troubled—and maybe you did not intend this literally—when you said that the Visas Viper group at the embassies only meet about once a month. I presume that if, somebody walks into an embassy and has significant information about an individual, a concern of being a terrorist, that the consular officer will not wait for the next monthly meeting. Right?

Ms. JACOBS. That is exactly right. Officers will send in individual cables if something comes to their attention before the monthly meeting.

Chairman LIEBERMAN. Thank you. That is very encouraging. I appreciate it.

The last witness on this panel is Secretary Morton, who is, as we well know, head of Immigration and Customs Enforcement (ICE). Let me just tell you before you begin, Secretary Morton, that yesterday we had a hearing here on the violence in Mexican and cross-border violence and its impact on our homeland security. And I want to thank you and congratulate you for the indictments that were issued, I guess last week, through the work of your people in ICE and the U.S. Attorney in Arizona and the work of, I gather, law enforcement around the country to bring to justice dozens of people involved in smuggling of people from Mexico into the United States. So I appreciate that work. Thank you.

TESTIMONY OF HON. JOHN T. MORTON,[1] ASSISTANT SECRETARY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MORTON. Well, thank you, Mr. Chairman and Senator Collins. That was an extraordinary case. It was in the making for well over a year. On the day of the arrests, we had over 800 Federal, State, and local law enforcement officers engaged in the searches and the arrests, and I am quite happy to say that we had the full and coordinated cooperation of the Federal police in Mexico, the Secretariat of Public Safety, which was extraordinary. They actually arrested one of our three main smuggling targets, so it was a good day for law enforcement.

Chairman LIEBERMAN. Good work. Thank you.

Mr. MORTON. Thank you very much for inviting me to address ICE's role in securing the visa process. Let me start by noting that

[1] The prepared statement of Mr. Morton appears in the Appendix on page 475.

good visa security is a multi-agency process that begins obviously before issuance and continues all the way through compliance by the visa holder with the terms of admission.

Done properly visa security facilitates lawful trade and travel—which I completely agree is a privilege, not a right—and while prohibiting the travel and entry of terrorists and others who would do harm to our Nation.

ICE plays many important roles in promoting the integrity of the visa process both before and after issuance. For example, we investigate and prosecute a wide range of visa fraud, and we use our administrative powers to remove visa overstays. I would like to obviously focus my remarks here today on our efforts to promote the security of the visa issuance process itself.

In that context, as the Committee well knows, our primary role is to run the Visa Security Program at U.S. embassies and consulates overseas. As you may know, we are the second largest criminal investigative agency in the Federal Government, and we have a very significant international presence overseas because so much of our mission is focused on investigating transnational crime—crimes such as money laundering, counterfeiting, and piracy of U.S. goods, international child exploitation, and the smuggling of drugs, arms, and people.

Under the Visa Security Program, ICE agents posted overseas add a very important layer to the integrity of the existing visa issuance process. In particular, experienced—and I place an emphasis on that—ICE investigators provide expert advice and training to consular staff. We review and scrutinize individual visa applications, and we conduct in-depth investigations when warranted.

An important point to keep in mind is that the VSP is not just a screening program; rather, it is an additional review process that complements the consular adjudication conducted by the Department of State and permits in-depth, on-site analysis and investigation of individual visa applications. This is not something that can be done remotely. To conduct a thorough investigation of a suspect application, an ICE agent needs to be able to interview the visa applicant in person, locate and research local records, and coordinate with foreign officials. In short, hard analysis and investigation require an on-site presence.

Indeed, depending on the concerns behind a given visa application, an ICE agent's investigation might prove quite complex and take literally a matter of months. Given our focus on national security, we do not send new recruits to VSUs. On the contrary, we assign experienced agents who have spent years developing interview, interrogation, and other skills while investigating crimes in the United States and overseas.

To date, the Visa Security Program has worked very well in the 14 posts where it has been implemented. Indeed, in our experience the consular staff at VSU posts have rapidly recognized the value of having ICE agents assist them and have not viewed the program as wasteful or distracting. This past fiscal year, our VSP units, working with our consular colleagues, screened over 900,000 applications and determined that 300,000 needed further review. Following investigation, and, again, in close consultation with the Department of State, we ultimately recommended to consular officials

to refuse over 1,000 of these applications. I am happy to report that in every single instance the Department of State followed our recommendation.

It is important to note that we do not view ourselves as overlords or competitors to consular officials. Our mission is to work with the consular team to identify questionable applications and to augment the State Department's ability to investigate and resolve issues of concern. ICE and the Department of State have jointly identified, as the Chairman has noted, 57 diplomatic and consular posts that warrant a Visa Security Unit. We are presently in 14 of these posts, and I anticipate expanding to four more in the remainder of this fiscal year and one in early 2011.

I am also working with Assistant Secretary Jacobs to address some of the implementation challenges both Departments face with regard to VSU so that we can improve the expansion process. And I want to just make a personal note here to say that I have found Assistant Secretary Jacobs to be quite willing to work with us and quite professional in her dealings, and I am confident that some of the implementation challenges that we may talk about here in a bit can be and will be resolved in a way that is good for both Departments and the country.

Please know that I am a strong supporter of the Visa Security Program and ICE's international investigative efforts generally. I am committed to ensuring that the program works well, as intended by Congress, as part of the Department of Homeland Security's broader security efforts, and to work with the State Department to expand the program in a thoughtful, efficient way.

Again, I thank you for the opportunity to appear before you once again, and, of course, I am happy to answer any questions the Committee may have, Senator Voinovich as well.

Chairman LIEBERMAN. Secretary Morton, thank you. We will do 7-minute rounds of questions.

Let me begin with the Visa Security Program. At an earlier hearing I raised the question about whether the entire Visa Issuance Program should go over to the Department of Homeland Security. That is probably not feasible or a good idea in the end, but I think the Visa Security Program creates a partnership here where the kind of concerns we have about the security implications of visa issuance and, frankly, the heightened security implications of visa issuance since September 11, 2001, can be taken care of. But, obviously, the program has not been sufficiently implemented, and that is what concerns us on the Committee.

Secretary Jacobs, I take it—well, let me ask you: What value does the State Department believe the Visa Security Program has?

Ms. JACOBS. Thank you, Senator. I think that at the posts where we have Visa Security Units, there has been a very good partnership between the consular officers doing visas and the visa security officers. They are able to look at applications. They have access to law enforcement sensitive information that sometimes it takes us a little bit longer to access. They bring a special expertise to the process where maybe answers do not make sense or certain things about the application raise questions. And so the consular officers have learned to work very closely with the visa security officers, to

listen to them. They know that they bring this expertise to the table, and I think it has been a very good relationship.

There have been cases the VSU officers have identified. You heard that there have been recommendations to refuse visas that have been followed.

Chairman LIEBERMAN. Every one.

Ms. JACOBS. So I think it is a very good partnership.

Chairman LIEBERMAN. So let me ask if my staff and I are right in citing at least seven cases where the chiefs of mission have objected to having people in the Visa Security Program in the consular office. Is that correct?

Ms. JACOBS. I am not sure of the exact number, but I do know that, yes, there have been instances where a chief of mission has denied a National Security Decision Directive 30 request.

Chairman LIEBERMAN. Why? What are the reasons why they would do that?

Ms. JACOBS. Well, actually, it is not really specific to the VSUs. Chiefs of mission have to look at a variety of issues for any agency, including the State Department, when we want to add new people to a mission. They have to look at the mission, why they are there. They have to look at the security situation in a given country. Is this a place where we are trying to keep the U.S. presence at a minimum? They actually have to think about things such as actual space limitations. Many of the VSUs are co-located in our consular sections, which in many countries are very tight right now. And so they have to look at all of these things.

They also look at the other agencies at post, and they look at what the VSU's goals and objectives are, and they make a determination about whether they think they already have that kind of expertise at the mission.

So there is any number of considerations given to these requests, and I must say that the initial answer sometimes is no, even for the State Department when we are trying to add consular officers to an embassy. But that is not the final answer. There is negotiation that normally takes place. Sometimes it is just a matter of clarifying exactly what it is that the new people will do at the embassy.

So it is a process that is worked through, but, again, it is not any chief of mission sort of singling out a Visa Security Unit to say, "I do not want you here." It is all of those things that are taken into consideration.

Chairman LIEBERMAN. Yes. Well, let me say that since, as I understand it, both the Department of State and the Department of Homeland Security through ICE have jointly agreed on the 57 posts where there should be a Visa Security Program, I really want to urge you to not find any excuse acceptable by the chiefs of mission for not having a Visa Security Program because this is so central to our homeland security. Will you take that back? I mean, there is certainly nothing in the law as we created it that gave the Ambassadors veto over location of a Visa Security Program that the two Departments have determined is in our national security interest.

Ms. JACOBS. Yes, sir. I am happy to take that back. Please know, though, that I am fully committed to try to make this program

work. I think from a very early stage the Bureau of Consular Affairs has supported the Visa Security Program. We had a senior officer at the Ambassador level who used to travel with the teams as they went abroad to try to make their case. It is something that, we encourage chiefs of mission to approve. There will always be, I think, at certain posts reasons that they cannot say yes, and sometimes it really is simply that they just do not have room. But you can count on Consular Affairs to really be supportive in this effort, and also as Assistant Secretary Morton said, the two of us are working together very closely to figure out ways to make this happen.

Chairman LIEBERMAN. Yes. Look, I accept your good will here and intentions. I am saying please take back both to the Department and then to any individual case where a chief of mission says, "No, I do not want the Visa Security Program," even for a reason that is not, personal but just "I do not have room," that they have to find room. This is that important.

Secretary Morton, my time is running out, but do you want to get into this generally from the DHS point of view?

Mr. MORTON. Yes. The challenges that we face in implementation are pretty much as Assistant Secretary Jacobs outlined them. Obviously, we have had some difficulties, and they have largely centered around concerns or objections from the Ambassador. Space and the overall size of the embassy is a common theme. There have been at times concerns that the Visa Security Unit is either not necessary or might duplicate something that the Ambassador feels his own staff or her staff could do.

What we have been able to do, however, is to go back—and obviously my view is quite similar to yours—and explain this is a statutory obligation, this is a statutory program, and we do have a joint list where both Departments have identified there are 57 posts that we need.

Chairman LIEBERMAN. Right.

Mr. MORTON. And things are much better. Assistant Secretary Jacobs has truly been working quite hard, and a lot of it is just an education process. But I think both Departments recognize we need to move with a little more dispatch on the implementation, and from the two of us you have that commitment. I personally went to London myself to make sure that the approval would be given to us by the embassy, and fortunately, the embassy did give it to me when I went myself.

Chairman LIEBERMAN. Good for you. I appreciate it. Look, what I am saying is—and I know Senator Collins shares this view—we are prepared to be the bad cops here. This is really important, and we are counting on you to make sure it happens.

Senator Collins, I have to go to the anteroom to take a call. I am going to leave you with power of the gavel with full confidence while I am gone.

Senator COLLINS. Thank you. You know I love that.

Chairman LIEBERMAN. Yes. [Laughter.]

Senator COLLINS [presiding]. Thank you, Mr. Chairman.

Let me follow up on the point that the Chairman just made. First, let me associate myself with his concerns about the resistance that you sometimes meet in trying to establish these security

units. I know London has been a particular problem. I salute you for solving that one. But the idea that there is resistance on this is really troubling to me.

There is another issue, however, and that is, the President's budget request for the Visa Security Program for fiscal year 2011 is the same as for this year. It is flat. So how can the Department intend to expand to more overseas consular posts with a flat budget?

Mr. MORTON. Well, let me start by saying that, as you know, at the time of the formulation of the 2011 budget, I was not the Assistant Secretary because I was preparing for the confirmation hearings before you and Senator Lieberman at that exact time.

What I can say is this: We are going to expand to the four. We are going to expand to at least one more in 2011. You can rest assured that there is not going to be a penny appropriated to us for visa security that will not be spent, and my foot is in the path. I will expand the program, working with Ms. Jacobs, as much as I can within the resources that I have, both specifically appropriated for Visa Security Units and our general international affairs budget. I do not want there to be any doubt about whether I support the program as enacted by Congress and the appropriations that we have been given. They are in many instances, fortunately, og us being given 2-year money, so I have some flexibility both this year and next, and I am going to spend every penny of it.

Senator COLLINS. I think it is important to note that Yemen is one of the countries where we do not now have a unit. Clearly, there needs to be one in Yemen. I know that is on your list for expansion. I would also note that Nigeria is another that is on the list and where we do not have a VSU.

It seems to me you need to be better resourced in order to establish these units, that it is not just a matter of the resistance that you inexplicably encounter at times from the Ambassador. There is a resource problem, and I know the Chairman and I will work with you to try to solve that problem.

Secretary Jacobs, I want to go back to you and ask you a series of questions to make sure that I understand what the Administration's policies are on revoking the visas of individuals who are on the various terrorist watchlists. And let us start with the TIDE list, which is the broadest, biggest terrorist database. Is there now an ongoing policy whereby the government continually checks the names that are on the TIDE list to see if they hold visas?

Ms. JACOBS. In the aftermath of the attempted bombing on Christmas Day, there was a complete scrub of TIDE files to see if any individuals in that database held visas. As a result of that, yes, we did discover people who had visas——

Senator COLLINS. Excuse me for interrupting, but my question is different. I acknowledged in my opening statement that scrub was done after the Christmas Day bomber. Is there now an ongoing check of those names? Because new names are going on that list every single day, literally hundreds. So is there an ongoing check?

Ms. JACOBS. There is an ongoing check of the TIDE files. There is still a review underway, if you will, of what exact procedures are going to be standard procedures will be for those constant reviews of the TIDE files.

I can tell you for the small percentage of TIDE files that come from Visas Viper information or cables, the procedure I explained to you earlier where we will be looking at those and revoking visas of people who have visas. But the TIDE files are very extensive, if you will, with regard to the type of information on any given individual. It can range from sometimes a poison pen letter to something that is very serious. And so when we send names in to NCTC to create a TIDE file for the part that we play a role in, we certainly have new procedures in place. For the more extensive files, I know that they are looking at the standards for watchlisting people, so all of those files would be looked at to see if names should be promoted over to the Terrorist Screening Center. But, again, it is such a variety of information, it is hard to say that, everyone in TIDE should automatically have the visa revoked.

Senator COLLINS. Well, it seems to me that everybody in TIDE ought to be identified and then brought in for an interview and a determination made. But let me switch to the terrorist watchlist. I know with the TIDE list there may be unverified information; there may be derogatory information that is not true. But the terrorist watchlist is a subset of the TIDE list where there has been some additional verification done. So it is a smaller, more reliable, if you will, list.

I was shocked to learn from the GAO that 1,150 people on the terrorist watchlist as of Christmas Day had valid U.S. visas. Of these individuals, how many have had their visas revoked?

Ms. JACOBS. These are the people on the terrorist watchlist?

Senator COLLINS. Correct.

Ms. JACOBS. I believe that all of the visas have been revoked except in cases where it was determined that it was somehow in the U.S. national interest to have someone keep a visa—in other words, someone who would have a waiver. That would sometimes be a head of State, oftentimes diplomats. Sometimes there are people who had been invited by a U.S. Government entity to come to the United States. And in those instances, we have waivers, and it is well documented and known why the person is allowed to come. But in other cases, the visas have been revoked.

Senator COLLINS. So absent those extraordinary circumstances, you are assuring our Committee that those 1,150 people have had their visas revoked?

Ms. JACOBS. Yes, ma'am.

Senator COLLINS. Thank you. Senator Voinovich.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you. I want to hit the Christmas Day situation real quickly. One, it has to do with having the right people with the right knowledge and skills at the right place at the right time. Two, it was a communications screw-up—we have had two hearings on this. Three, someone has said that they did not have enough information to stop the individual from coming into the country.

What I would like to know is: What information did they have? Who made the decision? And in this whole process was anyone fired, suspended, or reprimanded? You do not have to answer that today, but I would like the answer to those questions I just asked.

But the main thing I want to concentrate on is this: In 2007, this Committee enacted legislation that improved the security of the Visa Waiver Program and allowed new countries to join the program. We improved the program security by requiring participating countries to maintain a low visa refusal rate, issue secure electronic passports, report all lost and stolen passports to the United States, submit to periodic security reviews by the United States, accept repatriation of nationals, and share information on travelers who may pose a terrorist or criminal threat to the United States. All 36 of these countries are issuing machine-readable biometric passports today, and we are getting lost and stolen passport data from all the countries.

I do not believe that we would have had what we are getting today without this visa waiver legislation that enhanced what was being required from some of the countries. As a matter of fact, many of the countries that are in the program today have not complied yet with some of the new requirements that we have required in this legislation.

It is interesting to note that the last country that went in is Greece. I thought Greece would be one of the first countries to go in. In fact, they were qualified but for the fact that they refused to sign and ratify required information-sharing agreements. Finally they did it, and they were just recently admitted.

But one of the things that this Committee ought to know is that Greece was holding up a Mutual Legal Assistance Treaty, a critical law enforcement tool for the United States, between the United States and the European Union because they were holding out. And I honestly believe that had it not been for this Visa Waiver Program, that agreement would not be signed today.

In terms of public diplomacy, Ms. Jacobs, when I was in Latvia, President Zatlers told me that when it was announced that the Visa Waiver Program was coming to Latvia—Admiral Mullen was in town—it said it blew Mullen off the front page and it was just the Visa Waiver Program that was talked about. From a public diplomacy point of view, this has been a big hit.

I met recently with ambassadors from the Western Balkans. All of them are really interested in this program. But the problem is the program has come to a screeching halt, period, end of it. We go back to the 3-percent requirement. And the reason for it, Madam Ranking Member, is the fact that there was a provision put in the law that said that we had to come up with a biometric air exit system. The fact of the matter is that the Department of Homeland Security—and I am on the Appropriations Committee—has not requested any more money for this program. The little money they have, they have not spent. I met with the person that was heading up Customs and Border Protection. He said the program is not needed.

What I am trying to do is to find out from you: Is the air exit system fundamental to making this program the program we want it to be? Or, in the alternative, is there something else there that is getting the job done? And I am not getting an answer from you on it, because if you come out and tell us it is not needed and you do not want to spend, I think it is, millions and millions on putting this air exit program in place, then it is not necessary, and we

ought to know that. And if we do know it, I would ask Madam Ranking Member and others to maybe look at this and amend the statute so we can go back to what we had before and we can keep moving with this program that I think is enhancing the security of the United States of America and also something that is extremely important to this country's public diplomacy relationships with many countries who are our friends, who have people in Afghanistan and are helping us all over the world.

Mr. HEYMAN. Senator Voinovich, I would like to first agree with you. I thank you for your leadership on the Visa Waiver Program. In my full statement, we acknowledge the exceptional work that Congress has done to put in the provisions that you mentioned, to improve security, to enhance our information sharing, and to provide a basis by which not only do we benefit from enhanced immigration and customs security, aviation security, but also public diplomacy, as you mentioned.

In terms of the challenges we face, we are pursuing aggressively concluding the information-sharing agreements that Congress has requested. Those agreements are important, particularly in light of December 25, where those who may be unknown to us, may be known to our partners, and the information that they have may benefit our ability to do security here and in the aviation system.

As it pertains to a biometric exit, you are correct. The requirement for—the ability for the Secretary to waive the requirement of a 3-percent minimum for visa refusal for countries that are interested in the Visa Waiver Program was not met in June of this past year, and, therefore, we are unable to allow those who have over 3 percent designated into the program.

Senator VOINOVICH. The law provided—it was up to 10 percent.

Mr. HEYMAN. I believe that the 3-percent minimum up to 10 percent was the waiver ability unless we put in place a biometric air exit. Because we have not put in place biometric air exit, it is now back to the 3 percent.

That being said, we have now done a number of pilots to look at air exit, and we are looking at right now, as you said, the substantial costs that it would require to put this in place, the law enforcement interests that we have, particularly for those who we may capture leaving the country who are perpetrators of serious crimes, and the implications to questions of overstays.

I am pleased to tell you today that until recently we have had a very difficult time looking at the visa overstay data. We have just implemented a manual process that has allowed us to get greater fidelity into the overstay records, and I can confidently say that all of the countries that we have reviewed so far are far under the 2-percent overstay that we have looked at. We are going to complete that, but I think looking at the overstay data in a much more comprehensive way will provide us additional means for looking at Visa Waiver Program——

Senator VOINOVICH. Well, the main thing is this—I am leaving at the end of this year. If it is needed, let us appropriate the money for it. I put $50 million in the Homeland Security appropriations bill last year. You did not even ask for it this year, so somebody over there must think it is not needed. If it is not needed, let us know that it is not needed and what you have in place that you

think takes care of it without spending this enormous sum of money. And if you do that, then we can take it into consideration as to whether or not it is required or not required, and we can move on with it.

Mr. HEYMAN. Well, Senator, I would be happy to follow up with you. We are, I think, very close to finding a path forward, and we will be happy to follow up with you on that.

Senator VOINOVICH. Thank you.

Chairman LIEBERMAN [presiding]. Thank you, Senator Voinovich. Senator McCain, good morning.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Thank you, Mr. Chairman, and I thank the witnesses for being here.

Mr. Morton, I would like to talk immigration with you and the role that ICE has in this effort. I am sure you are aware that 45 percent of all apprehensions of illegal immigrants in this country occur in Arizona.

Mr. MORTON. I am indeed.

Senator MCCAIN. Sheriff Dever, who was here yesterday, said that law enforcement estimates that they catch about one out of every three to five illegal border crossers. Is that in keeping with your assumptions?

Mr. MORTON. Not those exact figures, but there is no question that, we estimate that roughly one out of every two people that comes to the United States unlawfully comes through Arizona. That is the single busiest corridor in terms of illegal immigration.

Senator MCCAIN. So lets say that this low estimate is right and one out of every three are apprehended, that would give you somewhere around 700,000, 800,000 people coming across our border illegally every year. Is that pretty much in keeping with the information that you have?

Mr. MORTON. I hesitate only because obviously the Border Patrol and not ICE is responsible for the apprehensions along the border, so I just do not want to steer you wrong on statistics. I deal with it more from the macro level. We have an estimate of anywhere between 10.8 and 12 million or more people who are here unlawfully, and that Arizona is obviously one of the major corridors for that.

The number does fluctuate. Obviously one of the questions is how much of that is due to enforcement and how much of that is due to economic difficulties. But there is no question that Arizona is a very busy corridor of illegal immigration.

Senator MCCAIN. Well, the President's budget requests $53 million less than 2010 for the identification and removal of criminal aliens. Can you explain the Administration's reasoning for this decrease?

Mr. MORTON. I am not aware of that reduction. I can only speak to that in terms of ICE's budget. Our budget, we have a very modest increase, and the areas of increase are largely for our Border Enforcement Security Teams—we hope to add three—and some additional resources for our detention system. It is largely keeping the present enforcement operation we have in place fully funded.

I will say, Senator McCain, again, from ICE's perspective, a quarter of all of our agents and officers are along the Southwest

Border. There has never been a time in our history when there were more ICE agents or officers, and the same is true for the Border Patrol along the four States.

Senator MCCAIN. Well, I think you just made a case for an increase in Arizona and across the Southwest Border, because if half the illegal immigrants are coming across in Arizona and only one-fourth of your agents are deployed there, it would argue for an increase in agents.

Mr. MORTON. The one-fourth figure is for all four Southwest Border States, and for Immigration and Customs Enforcement, it is particularly striking in that we have pronounced responsibilities both at the border and in the interior of the United States and in 44 countries overseas.

But let me assure you, there is no question that we are focused on this issue. We are, as we speak, the primary Federal agency assisting Cochise County with the murder of Mr. Krentz, the rancher. I came back from Arizona on Thursday where we announced the single largest alien-smuggling operation we have ever conducted in our agency's history, arresting roughly 50 defendants for organized alien smuggling on a grand scale through Arizona.

Senator MCCAIN. I am aware of that, and I wanted to congratulate you, and not only ICE but also the coordination between all levels of law enforcement in that operation. And I want to thank you for your leadership.

Can we talk about Operation Streamline for a minute with you? The law enforcement people tell me down on the border that the incarceration of 15 days, 30 days, 60 days, whatever it is, has had a significant effect on reducing the, I guess, maybe recidivism or the re-apprehension of individuals crossing the border. Has that been your experience?

Mr. MORTON. Yes, but let me caveat that Operation Streamline is a Border Patrol and U.S. Attorney operation. ICE is not directly involved in Streamline. I do understand from the Department of Justice and the Border Patrol that the rates of apprehension in those districts where Streamline is carried out are——

Senator MCCAIN. You do the detention, right?

Mr. MORTON. We do the detention, and we do all the criminal investigation. So the Border Patrol is the inspection and interdiction function; we are the Department's criminal investigators, and we carry out the detention function.

Senator MCCAIN. And do you think it has been an effective program from your observations?

Mr. MORTON. Again, it is an observation from afar, but I understand that the Border Patrol and the U.S. Attorney view it as having been effective in those areas where it is carried out and that the rates of apprehension are reduced in those particular districts.

Senator MCCAIN. Tell me a little bit about the operation that was just conducted in a very effective fashion. Does that also alert you to the fact that this human trafficking is really well organized. We used to kind of have the vision of a citizen of a country south of our border, usually Mexico, wanting to go to the United States and work and make their way across the border. Yet it seems to me that this is one of the changes, along with the dramatic increase in violence—which, I would be very interested in hearing your

thoughts on. The *L.A. Times* reported that 22,000 Mexican citizens have been killed during President Calderon's presidency in the last 3 years. I believe that is what they quote. But, also, maybe you could comment on how well organized and how coordinated the drug cartels and the human traffickers are and the sophistication of their operations. I would be very interested in hearing about your view on that.

Mr. MORTON. You are absolutely correct, Senator. There is a vision of alien smuggling either as a Mom-and-Pop effort or as just somebody deciding I am going to make my way to the United States and I am going to walk, and I might get some guidance along the way, but it is going to be an individual effort. Those images do not match up with today's human smugglers, and that is what our operation in Arizona was all about.

This is extremely sophisticated. There are loose confederations of alien smugglers. It is not just a question of organized criminals working in Mexico and the United States. Some of these chains stretch all the way to China, and in this particular case, we apprehended a number of Chinese who had come through a many-month journey, going through various drop houses and all sorts of different countries, making their way ultimately up to Mexico and through.

What we see is that obviously many of the cartels control the routes of passage across the border, and alien smugglers will have to coordinate with them for rights of passage. It is organized crime in very simple terms. That is how we approach it at ICE. Human trafficking is very serious, and we approach it as organized crime, and we are going to investigate it and try to root it out wherever we can.

Senator MCCAIN. I know that my time has expired, but could I just ask again, how closely intertwined and coordinated are the drug cartels and the human smuggling people? It seems to me that if they are using the same routes, if they are using the same techniques, they are intertwined and not really separate challenges in a way.

Mr. MORTON. Well, good border enforcement requires aggressive investigation of the smuggling of people, money, arms, and drugs. And all of those things are quite related; particularly the arms, money, and drugs piece really go hand in hand.

The alien-smuggling chains in our experience are distinct, but because they are using many of the same routes and methods, and because the drug cartels often control many of the corridors, there is a relationship. We often will see movements of aliens being sacrificed for purposes of, avoiding Border Patrol enforcement for a larger aim of the drug traffickers getting drugs across the border. So there is a relationship. I do not want to say that they are the same organizations, but there is a correlation, and that is very much the way we treat this. This is fighting organized crime along the border, whether it is in the form of alien smuggling, drug trafficking, arms, or money.

Senator MCCAIN. I thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator McCain. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you. Welcome, one and all. It is nice to see you. Thanks for joining us today, and thanks for your presence and responses to our questions.

The bombing that was attempted on last Christmas Day, was another wake-up call for our law enforcement officials. For our intelligence agencies, it also served as a reminder that we still have gaps in the aviation security apparatus and that the enemy around the world continues at its efforts to attack us from a lot of different directions.

Without question, we have come a long way since securing our homeland since September 11, 2001, but I think we all know we have to continue to remain vigilant and to work together at all levels of government.

I have two questions to ask of you today. The first of those questions revolves around the Visa Waiver Program, which we have discussed at some length here this morning. This program has been expanded over the last 5 years, I believe, to include nine additional countries, and that means I think people in as many as 35 or 36 countries can now travel to the United States without a visa. I think they can stay here for up to, I am told, as many as 90 days for business or for tourism. I believe this program has provided a great benefit to our country and to those who visit our country.

Having said that, we all know that it could also pose a security threat by the second and third generation nationals who have been radicalized in too many instances and may end up wanting to do harm to this country and the people who live here.

How real is this threat? If it is real, what steps have been taken within the program that we are discussing here today to prevent the threat from being realized?

Mr. HEYMAN. Well, thank you, Senator. I believe that first we have 36 countries now, and we are very much appreciative of the congressional support to this program.

The security benefits that accrue as a result of some of the changes that we have put in place over the last several years, and particularly in light of December 25, are ones that I think will allow us in the long term to address the kinds of threats that you have discussed.

What we saw on December 25, was an individual who was in some sense not known to us, though should have been known to us, who traveled through the aviation system and had used effective concealment to deliver his device over Detroit. And the programs that we now have put in place since December 25—beyond the Visa Waiver Program to include the Visa Security Programs, the Visas Viper recurrent vetting, the watchlisting reviews, and within the Department of Homeland Security—the checks that we do against watchlists and other databases prior to departure have in a real sense improved the security that we have for the traveling public in aviation security.

Beyond that, we are also working internationally with our partners. The Secretary has traveled to four regional conferences to encourage and work with our international partners to improve the standards across the globe in terms of screening, in terms of infor-

mation sharing, in terms of capacity building. And we are continuing to work that international effort.

But in the Visa Waiver Program, the information-sharing arrangements that we are now negotiating with our partners in the long term will help us to build the kind of understanding that we have prior to departure to assess, as we do right now with watchlists and other databases, the security risks of individuals traveling to this country.

Senator CARPER. Thank you. Anyone else want to add a comment on that?

[No response.]

One other question, if I could. I am a firm believer—I suspect that you are, too—in using a layered approach of people and technologies to protect our homeland from our enemies. I believe that relying too closely or too narrowly on just one layer over another has the potential for opening the doors to future intelligence failures. We are actually seeing some of that already.

One of the areas that I believe we could do a lot better is with respect to training of our screening and consular workforces. I am referring to the screeners at our airports and the Foreign Service officers who issue American visas at our embassies and consulates abroad.

While investing in high-tech scanning equipment is important, these devices have a shelf life, as you know, and will eventually become obsolete. Investing in people to detect fraudulent immigrant documents or spotting suspicious passengers is vital to safeguarding our country.

Could each of you take just a moment to address those concerns and, if possible, to offer up to our Committee some steps that your agency is taking to improve screening processes? Ms. Jacobs, would you like to go first?

Ms. JACOBS. Yes, sir. Thank you for that question. I think you are absolutely right that proper training is crucial. In Consular Affairs, consular officers out doing visas really are the first line of defense in protecting our borders, and it is very important for those officers to be properly trained.

We put all of our new officers through a basic consular training program that includes 80 hours of security-related training, fraud detection, interviewing techniques, ability to look at documents to recognize things that sort of jump out as problems. We even train officers in how to detect deception, reading facial expressions.

We also have other agencies that come over to our Foreign Service Institute to talk to people. Our national security partner agencies' representatives come over to talk about threats, things to look at, red flags.

So it is there. It has been a very important part of our training always, but certainly after September 11, 2001, we are always looking for ways to improve that training. When an officer gets to a post, they undergo further training, and for the officers who are consular combed, who will stay doing consular work for most of their careers, there is an ongoing training program at every stage of their career to reinforce what we are doing.

In fraud prevention, we have come very far. We are using new technology. We are using off-the-shelf databases, like LexisNexis,

and other tools to check information. And now that we are going to an online visa process, we will actually get all of the data on our applicants in advance of an interview, and it is going to give us a chance to actually start data mining, looking at common addresses, common phone numbers, other things that should raise red flags for us. So that will also be, I think, another very important tool in our kit for having officers well trained to recognize fraud and other security-related issues.

Senator CARPER. Thanks very much for that response. Mr. Heyman.

Mr. HEYMAN. Thank you, Senator. I could not agree more. It is a principle of Homeland Security that we have to have defense in depth, to have layers of defense and not rely on any single solution to secure whether it is aviation or other important entities in our homeland.

In terms of aviation security, the layers begin with the travel document and the standards that are required to ensure that they are not fraudulently obtained or created. An individual must obtain that document. Then they may go through a visa process or an authorization process. There are visa security agents, as we have testified to today, as well as Consular Affairs and database checks for that layer.

Once an individual has that permission to travel to the United States, the next layer is the pre-departure checks that the Department of Homeland Security can do against passenger name records up to 72 hours in advance of a departure to see if there are any matches to the No Fly List, the watchlist, or other lists.

And then when they come to the airport, we have two different models. There is the domestic model in the United States which the Transportation Security Administration (TSA) of the Department of Homeland Security runs, and then there are the models abroad where the Department of Homeland Security does not have a role to play per se; security is managed abroad by the local entities there. But at home, we have behavioral detection officers. We have the screening, both advanced imaging technologies. We have other types of technologies to look at concealment. And then, finally, in-flight security to include air marshals, hardened doors, and things of that nature. All of these layers come together to perform aviation security.

In terms of training, each of the individuals who are on the front line there, whether it is a transportation security officer of TSA, whether it is a Customs and Border Protection official who is stationed abroad or working here in the United States, or visa securities officers, as Secretary Morton has testified, have not only extensive training but extensive in-field work as part of their training procedures.

One of the things we are looking to do as we look at improving international aviation security is the international standards to include training for capacity building, and that is one of the things we are seeking to work with the International Civil Aviation Organization (ICAO), through the United Nations, as we work with our partners abroad to improve standards around the world.

Senator CARPER. Thank you. My time has expired. Mr. Chairman, could Mr. Morton have just 30 seconds, just briefly to respond?

Chairman LIEBERMAN. Yes, of course. Go right ahead.

Senator CARPER. Very briefly, sir. Thank you.

Mr. MORTON. Well, I will beat a dead horse a little bit more and say that I completely agree with the idea, obviously, of a layered defense.

Very quickly, training is critical. The Act directly requires it of ICE in its role through the Visa Security Program. It is one of the things that I want to work with the State Department more on, and we are very cognizant of—we do not send, as I noted in my initial remarks, new recruits overseas to do this. We recognize that we are the largest investigator of visa frauds in the country, and so we have a great deal of experience with, figuring out if somebody is telling the truth or not to the government. We want to bring that experience, not just have training for consular officers, but to share what it is we do every day. And, we are in many respects the policer of that system, and we have a lot of expertise and thoughts on it.

Obviously, also in our role of policer of the system, we deal a lot with visa overstays. We see what kind of misrepresentations people make, patterns. We do this on a fairly large and grand scale. And so I am a big believer in not just having the Visa Security Program there to identify individual applications, but to help with the training of consular officers and to view this as a team effort.

Senator CARPER. Good. Thank you all very much for those responses, and thank you, Mr. Chairman, for your generosity.

Chairman LIEBERMAN. Not at all. Thank you, Senator Carper. It was an important question.

We will do another quick round. I would not call it a lightning round, but it will be a short round of 5 minutes each.

Let me come back just to ask a few more questions about the Visa Security Program. First, what is different about the review that you do before issuing visas in those 57 high-risk posts that you have identified as high risk as opposed to the others? What more do you do?

Ms. JACOBS. Well, where we have VSUs, basically all of the applicants are initially screened by a consular officer. They are run through a series of checks to include a check of our Lookout System. We also check their fingerprints against Automated Biometric Identification System (IDENT) and Integrated Automated Fingerprint Identification System (IAFIS). If there was any kind of Lookout entry that requires what we call a security advisory opinion, sending the case back, that will happen. And so all of those sort of initial screenings take place.

Where we have VSUs, the value-added is that a visa security officer then looks at the application, and if there is, for example, a law enforcement entry in the Lookout System, a National Crime Information Center (NCIC) hit, they can easily access the information behind that hit. They can also tell sometimes just by where people are going or just certain answers to questions because of their experience with what happens when people actually come to

the United States, they are able to go back to the consular officer and say, "You should be asking these additional questions."

So it is a give-and-take process. It is, if you will, another layer to the process during the visa stage.

Chairman LIEBERMAN. Mr. Morton, why don't you answer the question and I guess in a way focus it from your point of view. What is it that a visa security officer working as part of ICE brings to that review that the consular officer might not or does not do?

Mr. MORTON. I think in sort of common parlance, "what do we get from this," we get an ability to kick the tires and in a profound way, down to a level of an individual application. And we bring to bear an investigator, somebody who has spent their life—and as I said, we do not send new recruits, we send experienced people over there, typically from our international program. Already they have had experience living overseas, speaking the foreign language. And you get somebody whose job it is to uncover fraud and misrepresentation, who brings a gut sense as an investigator when something is not right, has much quicker access to the databases and to classified information, knows what to do when, there is a little smoke here or something does not add up, well, what do you do? Well, you are an investigator. That is what you are trained to do. And you know, we are going to go down to the courthouse and see whether or not you are really married to this person or that person or whether you got divorced. We are going to call our colleague in New York and say, "Does it seem odd to you that we would have 50 visas with the same address on this block being used?"

It is that kind of in-depth analysis and investigation that can be brought to bear with people who know what they are doing in that area, and it is in no way to suggest that consular officers are not quite competent with what they do. It is just recognizing that the adjudication process is different than the investigative process. And when you can mirror those powers, a lot of the screening can be done by the consular officers, but often it is their first or second tour, so they are relativley new in the scale of their work, and we are bringing some seasoned hands to, again, help kick the tires.

Chairman LIEBERMAN. Yes, well, that is a very good answer, what I thought was the case. The State Department personnel are Foreign Service officers, usually junior, very able, as I have met them, but not specifically trained—although they are carrying out some of these responsibilities in investigation with a focus in this case on counterterrorism and homeland security.

When we remember, in response to the Christmas Day bombing, one of the first things to be done was the subjecting of extra measures to those 14 countries. And now that is altered in a much more direct and intelligence-driven way. But I am in some sense both interested and encouraged that the list of countries which these two Departments, have designated as higher risk is way beyond 14. It is 57. I am encouraged by that because obviously we know that the Islamist extremist terrorist movement is operating, and others who want to threaten our security, operating globally.

So how did you make the judgment—and just a quick answer—about where to extend beyond that list of 14, which in a sense is the obvious first place to look? Secretary Morton.

Mr. MORTON. A lot goes into deciding those posts. Some of it I would prefer to give you a straight briefing on, but not in a public setting.

Chairman LIEBERMAN. That is fine. Sure.

Mr. MORTON. But London is a perfect example. You ordinarily do not think of the British being at the top of our list for having to worry about whether they are going to fly planes into buildings. On the other hand, when you understand the visa-issuing process and you realize that London is a place where many people other than British nationals are getting visas. Then suddenly you realize that it is very important from a national security perspective and needs to be on the list of 57, which it is. And so it is those kinds of things, looking at the opportunities for even if the nationals of a given country have a good record of compliance, is it a vulnerability with regard to nationals from countries next door? Are there corruption issues? There is a lot that goes into it, and that is how we come to 57.

Chairman LIEBERMAN. Good enough. Thank you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

In the aftermath of the Abdulmutallab case, there was some confusion over which agency considered itself ultimately responsible for revoking of a visa on terrorism grounds. And I remember the National Counterterrorism Center Director testifying before us and expressing his bafflement at some of the comments that were made by the State Department personnel.

The State Department spokesman, shortly after the Christmas Day bombing attempt, said the following: "It would be up to the National Counterterrorism Center to make the determination whether to revoke a person's visa or take other action."

When asked later by a reporter why the State Department did not revoke Abdulmutallab's visa, the State Department spokesperson said, "Because it is not our responsibility."

Secretary Jacobs, what is your reaction to those comments?

Ms. JACOBS. I believe that the response by the spokesman was probably a bit of a shortcut, if you will. I think what he was trying to say is that the way the process worked at that time prior to Christmas was that names would go into the NCTC, and if the NCTC felt that the name or the information met the standards at the time for promoting the name over to the Terrorist Screening Center watchlist, that needed to happen before we would have revoked the visa.

I think that is probably what he was trying to say. It did not come out exactly that way, I realize. The State Department has the authority and responsibility for revoking visas, and we take that very seriously, and as I have explained to you, we have new procedures in place now for more expeditious revocation after Christmas Day.

Senator COLLINS. Thank you.

Mr. Heyman, the Department of Homeland Security also has some authority in this area. Section 428 of the Homeland Security Act of 2002 provides DHS with broad authority to set visa policy. Specifically, it vests in the Secretary the exclusive authority to "issue regulations with respect to administer and enforce the provisions of law relating to the functions of consular officers of the

United States in connection with the granting or refusal of visas." It also says that the Secretary has the authority to refuse visas in accordance with the law.

Do you think there is confusion over the role of DHS in this area?

Mr. HEYMAN. In our partnership with the State Department, there does not appear to be confusion. As we have testified today, there are numerous instances, over 1,000 perhaps, where the Department has made recommendations to refuse or revoke a visa that have been readily adapted and responded to by the State Department. Those are recommendations. The Secretary has the authority to make those determinations on her own, though has not needed to——

Senator COLLINS. It has not been exercised.

Mr. HEYMAN. Not been exercised, and largely there is a good working relationship with the State Department, and we have not had a need to do so. And the Abdulmutallab case, had he arrived in Detroit, it is likely that we would have noted the derogatory information, gone to secondary, and perhaps made a recommendation to the State Department to revoke the visa.

Senator COLLINS. Do you believe that the Department has the authority to establish a visa policy that would require the suspension of all visas held by the individuals in the TIDE database pending further investigation?

Mr. HEYMAN. The Department has the broad authority to make policy on visa refusals or revocations. In the particular example that you give, through an interagency process, the government has already made a determination that individuals in TIDE are not eligible for terrorist watchlist and individuals—and beyond that, they are not on the No Fly and Selectee Lists since they are not even a resident in the terrorist watchlist.

As such, it would be questionable, I think, as to whether their visas required revocation. Some reasons that people are in the TIDE database, as was noted earlier, is because of poison pen letters or investigations have concluded fragmentary information, I am just speculating now. I would not necessarily jump to the conclusion that visas would need to be revoked just because somebody was there.

Senator COLLINS. But my question is not the desirability of the policy. It is trying to establish authority. Do you believe under current law that the Secretary would have the legal authority to issue regulations requiring such a policy?

Mr. HEYMAN. I would have to look at it more carefully. She has broad authority as stipulated in the Act, and so let me perhaps do a little bit more thinking on that and get back to you.

Senator COLLINS. Thank you. The final comment that I want to make concerns an issue that was brought up both by Senator Carper and Senator Voinovich, and that concerns the Visa Waiver Program. I think that it is unacceptable that fewer than half of the 36 countries currently participating in the Visa Security Program are now sharing all the information on dangerous individuals that is supposedly required to take advantage of that program. And I really think we are going to need to take a harder line on this.

It was supposed to be a condition of participation, and if countries are not willing to share that information with us, then I do not see how we can allow participation in a program that might result in one of their citizens coming to our country without having to get a visa and possibly do us harm.

So my final comment is to urge you to take a far harder line on the information-sharing agreements, and if countries are not willing to abide by that and share information with us, then we should kick them out of the Visa Waiver Program.

Mr. HEYMAN. Well, thank you, Senator. I share your interest, and these are important agreements that need to be concluded. We are, as I had mentioned earlier, focused on concluding these agreements. It is our top priority in the Visa Waiver Program right now. We have a number of ongoing negotiations to move forward as we speak, and we have a path to conclude all of these no later than 2012.

Some of the challenges we face in these arrangements are different legal systems, the ratification systems, perhaps the need for assurances on privacy, and we are working carefully through that with all of the countries, with, I think, good effect, and I think we are on a path hopefully, as you said, to move as fast as we can on this and no later than 2012.

Senator COLLINS. Thank you. It is still troubling to me that we are not even halfway there, and so a lot of work remains to be done. I know it is very difficult, but we are extending a benefit to the citizens of those countries.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins. Just to say for the record that I agree with you totally. I know this can be diplomatically sensitive because we are dealing in many cases, probably all cases, with countries that are allies and that are supportive of us in other ways. But, the refusal or slow walking in sharing information with us is really not acceptable because of the higher priority that we have to give to homeland security. So, again, we are happy to be cited as breathing down your neck next time you——

Mr. HEYMAN. So cited, sir.

Chairman LIEBERMAN. Thank you for this hearing. I appreciate very much some of the things that have been done since December 25. I say, Secretary Jacobs, particularly that you have this, I call it, software in place to avoid the problem with the misspelling of the name, and that the judgment by a consular officer that somebody may be a terrorist immediately will lead to revocation of a visa unless there is some other national security reason for not doing that.

I do want to emphasize that we are very concerned about the slowness and incompleteness of the placement of the visa security officers in those 57 high-risk posts, and I just want to urge you to do it, as we talked about before—and, Senator Collins and I have talked, and we are going to take it on ourselves to try to convince the Administration. Of course, we could use your help in that budget office, and our colleagues who are appropriators to give you the money you need to do that. That probably has as good a return on investment as a lot of other things we could do with the money.

But thanks for what you are doing every day. Thanks for your testimony today. We will keep the record of the hearing open for 15 days for additional statements or questions.

The hearing is adjourned.

[Whereupon, at 12 Noon, the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Joseph I. Lieberman
Homeland Security and Governmental Affairs Committee
"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
Statement for Intelligence Reform Hearing
January 20, 2010

Good morning. This past Christmas Day, as we all know, Umar Farouk Abdulmutallab slipped through the multilayered defenses we've erected since 9-11 to stop attacks against our homeland and boarded Northwest Flight 253 from Amsterdam to Detroit, on which he attempted a suicide bombing.

A faulty detonator and courageous and quick action by the passengers and crew prevented the deaths of the 290 people on board that plane and many more on the ground below.

We were lucky.

Because it has now been five years since the enactment of the 9-11 Commission recommendations for intelligence reform, Sen. Collins and I decided last year to initiate a series of oversight hearings this year to examine how well these reforms have been implemented and whether further changes in the law, regulation or implementation are needed to protect our country.

That is, in fact, the inquiry we begin today, but now, of course, we must carry out our oversight through the unsettling prism of the Christmas Day breach of our homeland defenses by the terrorist, Abdulmutallab.

The Intelligence Reform and Terrorism Prevention Act of 2004, commonly known as the 9-11 Commission Act, was the most sweeping intelligence reform since the creation of the Central Intelligence Agency more than 50 years earlier.

Among its many significant improvements, the 9-11 Commission Act established a Director of National Intelligence to integrate our 16 intelligence agencies.

It 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.

Earlier in 2002, our government's failures on 9/11/01 also moved Congress to act on recommendations to create a Department of Homeland Security to better cope with the threats our country would face in the 21st century.

I believe these post 9-11 reforms have worked very well.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00193 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.001

The record shows that after the creation of the Department of Homeland Security in 2002, and the establishment of the DNI and NCTC in 2004, there was not a terrorist attack by Islamist extremists on America's homeland for almost seven years.

No one would have predicted that on Sept. 12, 2001, so we have a lot to be grateful for.

Some of the most successful defenses of our homeland, in my opinion, have been truly amazing, although the details of these, of necessity, remain largely unknown.

Two of the most impressive of those successful defenses occurred in 2009, with the regard to Najibullah Zazi and David Headley.

One of the most impressive cases to me was the Zazi case, who was arrested last September with the plans and materials needed for bombing attacks in New York City.

This was the most dangerous terrorist plot on our soil since 9/11 and it only was foiled by brilliant, courageous and cooperative work of our intelligence, law enforcement and homeland security agencies.

Sen. Collins and I and other members of the Committee have been briefed on the details. But everything worked just was we hoped it would it would when we adopted the post 9-11 reform legislation. There was remarkable agility, brilliant judgment and total cooperation between intelligence, homeland security and law enforcement communities both here within the United States and throughout the world.

Notwithstanding these remarkable achievements over the seven years since the enactment of DHS, the record also shows that that in 2009, three Islamist terrorists broke through our defenses: Carlos Bledsoe, who murdered a U.S. Army recruiter in Little Rock, Arkansas, in June; Nidal Hassan, who murdered 13 Americans at Fort Hood in November; and Umar Farouk Abdulmutallab, who would have killed hundreds more if the explosive he had hidden in his clothing on Christmas Day had worked.

Clearly, some elements of our homeland defenses are not working as we need them to. We must find out what is going wrong and why and fix it.

I know it is probably not realistic to promise that we will stop every terrorist attack on our homeland, but that certainly must be our goal.

And that certainly is the standard that will guide our Committee in this inquiry, and the other we are conducting on the terrorist attack at Fort Hood.

Our purpose is to review the current state of our homeland security and in these cases to make recommendations for reform that will get our homeland as close as possible to 100 percent security from terrorist attack.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00194 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.002

In the Christmas Day bombing case, there was so much intelligence and information available to our government that pointed to Abdulmutallab's violent intentions that it was beyond frustrating – it is infuriating that this terrorist was able to get on the plane to Detroit with explosives on his body.

He was able to do so, as President Obama correctly has said, because of systemic failures and human errors.

We must fix the systemic failures that occurred in these latest attacks and if we – or the Administration, through its ongoing review – find that there were federal personnel who did not perform up to the requirements of their jobs, they should be disciplined or removed.

As is clear from the Christmas Day attack – which almost killed hundreds, the Ft. Hood attack – which did kill 13 – and the thwarting of the Zazi plot that saved countless American lives, the decisions of the public servants who work to protect us from terrorists every day have life and death consequences.

If we do not hold accountable those who made these human errors, the probability is great that they will be made again.

I have not called this hearing to knock down the new walls of homeland security we have built since 9-11, but to repair and reinforce them so they better protect the American people from terrorist attack.

It is in that spirit that I look forward to our witness's testimony.

Welcome Admiral Blair, Director Leiter, Secretary Napolitano. I thank you – and the men and women you lead – for your service to our country and for being here today.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00195 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.003

Opening Statement of
Senator Susan M. Collins

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"

Committee on Homeland Security and Governmental Affairs
January 20, 2010

★ ★ ★

Every day, the men and women of our military, homeland security, law enforcement, and intelligence community work to keep our nation safe. They serve on the front lines of the war against terrorism. Over the last year alone, their efforts have helped thwart numerous terrorist attacks.

But as the attempted Christmas Day attack demonstrates, our government's efforts to detect and disrupt terrorists' plots must be strengthened.

We dodged a bullet in the skies above Detroit on Christmas day. A mere fluke – a mistake by the terrorist aboard the plane or a failed detonator – prevented that attack from succeeding. The quick action of courageous passengers and crew helped spare the lives of the nearly 300 passengers on Flight 253.

We cannot escape these cold, hard facts: terrorists have not relented in their fanatical quest to frighten our nation's citizens and to slaughter as many Americans as they can. Their tactics continue to evolve. Attacks inspired by al-Qaeda's violent ideology, including those by "lone wolves" or those perpetrated by smaller uncoordinated cells, are incredibly difficult to detect. The threat posed by America's terrorist enemies continues to grow, and our nation's efforts to defeat them must be nimble, determined, and resilient.

In response to the terrorist attacks of September 11, 2001, this Committee authored the most sweeping reform of our nation's intelligence community since the Second World War. The Intelligence Reform and Terrorism Prevention Act of 2004 did much to improve the management and performance of our intelligence, homeland security, and law enforcement agencies. The increased collaboration and information sharing have helped our nation prevent numerous attacks – at least nine in the last year alone.

56838.004

But reform is not a destination; it is a work in progress. Reform requires constant focus and attention to stay a step ahead of the threats we face.

For example, despite vast improvements in information sharing, our intelligence community continues to rely on internal systems and processes that are relics from the days before reform. These systems do not effectively surface intelligence information so that analysts and security officials can effectively identify threats in real-time.

The President has asserted – and I agree – that there was ample, credible intelligence on Abdulmutallab to warrant his inclusion on the "No Fly" list. Yet that did not occur, even though his father warned U.S. officials about his ties to Islamist extremists. Whether this failure was caused by human error, poor judgment, outmoded systems, or the sheer volume of data that must be analyzed, we must develop systems and protocols that prevent these failures.

Consider what I believe to be the most obvious error in handling Abdulmutallab's case: after his Islamist extremist connections in Yemen were reported by his father, the State Department should have revoked his visa. At the very least, he should have been required to come to an embassy and explain his activities before he was allowed to travel to the United States.

The State Department has this authority. In fact, the Intelligence Reform Act protects the Department from lawsuits when its officials revoke a visa overseas. But the State Department failed to act.

The President has now directed the Intelligence Community to determine which of the 400,000 suspected terrorists in the Terrorist Screening Center's terrorist watchlist have valid U.S. visas. But that response is not sufficient.

The government should immediately identify and suspend the visas of all persons listed in the broadest terrorist database operated by the NCTC, known as TIDE, until a further investigation is undertaken in each case. These visa holders with suspected connections to terrorism should shoulder the burden of proving they do not intend to harm this nation or its citizens. If they cannot meet this burden, then we cannot take the risk of permitting them the privilege of traveling to our country.

56838.005

But immediately revoking the visas of suspected terrorists is only the first step. The Department of Homeland Security also should confirm the validity of the visa of every foreign passenger that attempts to board an airplane to this country rather than waiting until the arrival in our country. There is no technological reason this cannot occur – we already confirm whether a passenger is on the No Fly or Selectee list.

We did not choose this war. It was thrust upon us by terrorists whose only mission in life is to destroy our American way of life. Our counterterrorism efforts must be tireless and steadfast. We must continue to build on the intelligence reforms already in place to make America more secure.

# # #

56838.006

Senate Homeland Security and Governmental Affairs Committee

20 January 2010

Intelligence Reform: The Lessons and Implications of the Christmas Day Attack

Statement for the Record

of

Dennis C. Blair

Director of National Intelligence

Michael E. Leiter

Director of the National Counterterrorism Center

Statement for the Record

20 January 2010

Senate Committee on Homeland Security and Governmental Affairs
"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"

Chairman Lieberman, Ranking Member Collins, and Members of the Senate Committee on Homeland Security and Governmental Affairs: Thank you for your invitation to appear before the committee to discuss the counterterrorism efforts of the Intelligence Community and the improvements underway to fix deficiencies.

It is my privilege to be accompanied by Janet Napolitano, Secretary of Homeland Security, and Michael Leiter, Director of the National Counterterrorism Center.

The attempted terrorist attack on Christmas day did not succeed, but, as one of several recent attacks against the United States inspired by jihadist ideology or directed by al Qa'ida and its affiliates, it reminds us that our mission to protect Americans is unending.

Let's start with this clear assertion: Umar Farouk Abdulmutallab should not have stepped on that plane. The counterterrorism system failed and I told the President we are determined to do better.

Within the Intelligence Community we had strategic intelligence that al Qa'ida in the Arabian Peninsula (AQAP) had the intention of taking action against the United States prior to the failed attack on December 25th, but, we did not direct more resources against AQAP, nor insist that the watchlisting criteria be adjusted prior to the event. In addition, the Intelligence Community analysts who were working hard on immediate threats to Americans in Yemen did not understand the fragments of intelligence on what turned out later to be Mr. Abdulmutallab, so they did not push him onto the terrorist watchlist.

We are taking a fresh and penetrating look at strengthening both human and technical performance and do what we have to do in all areas. I have specifically been tasked by the President to oversee and manage work in four areas:

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00200 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.008

Immediately reaffirm and clarify roles and responsibilities of the counterterrorism analytic components of the IC in synchronizing, correlating, and analyzing all sources of intelligence related to terrorism.

Accelerate information technology enhancements, to include knowledge discovery, database integration, cross-database searches, and the ability to correlate biographic information with terrorism-related intelligence.

Take further steps to enhance the rigor and raise the standard of tradecraft of intelligence analysis, especially analysis designed to uncover and prevent terrorist plots.

Ensure resources are properly aligned with issues highlighted in strategic warning analysis.

NCTC has been tasked by the President to do the following:

Establish and resource appropriately a process to prioritize and to pursue thoroughly and exhaustively terrorism threat threads, to include the identification of appropriate follow-up action by the intelligence, law enforcement, and homeland security communities.

Establish a dedicated capability responsible for enhancing record information on possible terrorist in the Terrorist Identities Datamart Environment for watchlisting purposes.

The Events Leading Up to the Christmas Day Attack

I will now briefly discuss some of the details of the bombing attempt and what we missed. As the President has said, this was not—like in 2001—a failure to collect or share intelligence; rather it was a failure to connect, integrate, and understand the intelligence we had.

Although NCTC and the Intelligence Community had long warned of the threat posed by al Qa'ida in the Arabian Peninsula—to include as Director Leiter did with this Committee just this past Fall—we did not correlate the specific information that would have been required to help keep Abdulmutallab off that Northwest Airlines flight.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00201 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.009

More specifically, the Intelligence Community highlighted the growing threat to US and Western interests in the region posed by AQAP, whose precursor elements attacked our embassy in Sana'a in 2008. Our analysis focused on AQAP's plans to strike US targets in Yemen, but it also noted—increasingly in the Fall of 2009—the possibility of targeting the United States. We had analyzed the information that this group was working with an individual who we now know was the individual involved in the Christmas attack.

In addition, the Intelligence Community warned repeatedly of the type of explosive device used by Abdulmutallab and the ways in which it might prove a challenge to screening. Of course, at the Amsterdam airport, Abdulmutallab was subjected to the same screening as other passengers—he passed through a metal detector, which didn't detect the explosives that were sewn into his clothes.

As I have noted, despite our successes in identifying the overall themes that described the plot we failed to make the final connections—the "last tactical mile"—linking Abdulmutallab's identity to the plot. We had the information that came from his father that he was concerned about his son going to Yemen, coming under the influence of unknown religious extremists, and that he was not going to return home. We also had other streams of information coming from intelligence channels that provided pieces of the story. We had a partial name, an indication of a Nigerian, but there was nothing that brought it all together—nor did we do so in our analysis.

As a result, although Mr. Abdulmutallab was identified as a known or suspected terrorist and entered into the Terrorist Identities Datamart Environment (TIDE)—and this information was in turn widely available throughout the Intelligence Community—the derogatory information associated with him did not meet the existing policy standards—those first adopted in the summer of 2008 and ultimately promulgated in February 2009—for him to be "watchlisted," let alone placed on the No Fly List or Selectee lists.

Had all of the information the U.S. had available, fragmentary and otherwise, been linked together, his name would have undoubtedly been entered on the Terrorist Screening Database which is exported to the Department of State and the Department of Homeland Security. Whether he would have been placed on either the No Fly or Selectee list—again based on the existing standards—would have been determined by the strength of the analytic judgment. One of the clear lessons the U.S. Government has learned and which the Intelligence Community will support is the need to modify the standards for inclusion on such lists.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00202 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.010

In hindsight, the intelligence we had can be assessed with a high degree of confidence to describe Mr. Abdulmutallab as a likely operative of AQAP. But without making excuses for what we did not do, I think it critical that we at least note the context in which this failure occurred: Each day NCTC receives literally thousands of pieces of intelligence information from around the world, reviews literally thousands of different names, and places more than 350 people a day on the watchlist—virtually all based on far more damning information than that associated with Mr. Abdulutallab prior to Christmas Day. Although we must and will do better, we must also recognize that not all of the pieces rise above the noise level.

Intelligence Community Reform

While the December 25 attempt exposed improvement needs and flaws in coordination, it also revalidated the importance of intelligence efforts underway. The Intelligence Reform and Terrorism Prevention Act of 2004 and the progress of the past five years will continue to guide our future improvements. Let me acknowledge up front the vision and tenacity of Chairman Lieberman, Senator Collins, and the Members of this Committee as you developed and passed the 2004 Intelligence Reform Act. We share the goals you laid out in that legislation. The shortcomings that have been identified as a result of the December 25 attempt should not obscure the progress the Intelligence Community has made in improved collection and analysis capabilities, in improved collaboration and in sharing information, both against al Qa'ida and against the many other threats to our national security.

The United States Intelligence Community must constantly strive for and exhibit three characteristics essential to our effectiveness. The IC must be integrated: a team making the whole greater than the sum of its parts. We must also be agile: an enterprise with an adaptive, diverse, continually learning, and mission-driven intelligence workforce that embraces innovation and takes initiative. Moreover, the IC must exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people.

The Intelligence Community has made significant strides in addressing the underlying deficiencies exposed by the attacks of 9/11. But, we must constantly improve and adapt.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00203 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.011

To confront constantly evolving threats, we have made many changes in the way we conduct intelligence, law enforcement, homeland security, diplomatic, and defense activities since 2001. A prime example of improved integration is the new level of cooperation among FBI, local law enforcement and U.S. intelligence agencies in the recent arrests of Najibullah Zazi and David Headley, Americans allegedly associated with foreign terrorist organizations who are charged with planning attacks in this country and overseas. In both cases, tips and leads were smoothly passed among those gathering information in this country and those gathering information overseas, including foreign intelligence services that provided information or responded to questions.

Like our armed forces and first responders, intelligence professionals are on the front lines in defense of this country. Their operations are already collaborative between and across agencies to an extent that was unheard of five years ago. Continued commitment and investment in this reform are vital. If we become complacent now, or pessimistic about future progress, and revert to stovepipes and turf battles, full transformation will never be achieved.

In the area of information sharing, let me address areas where we have made progress and are focusing our future efforts:

Policy: The Office of the Director of National Intelligence (ODNI) has continued the transformation of information sharing by implementing Intelligence Community Directive (ICD) 501, "Discovery and Dissemination or Retrieval of Information." This ICD mandates wide-ranging actions to enable information sharing, including the ability to discover and request information from all IC elements, who now have a "responsibility to provide" such information. Implementation of the Intelligence Information Sharing Dispute Resolution process, formulated to simplify and streamline information sharing, has also produced positive results.

The Information Sharing Environment (ISE). The ISE is comprised of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration. In collaboration with our homeland security partners, fusion centers are able to access needed intelligence information for their mission, and in situations of information sharing conflict, procedures are in place to resolve information sharing issues.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00204 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.012

Library of National Intelligence (LNI). The ODNI has made considerable progress on improving information sharing of finished intelligence across the IC through the creation of the LNI. The LNI is part of the DNI's efforts to build a more collaborative IC, improve information sharing, transform analysis, and modernize the IC's business practices. Access to LNI significantly improves access to critical expertise and the use of advanced tools to develop coordinated intelligence products.

Collaborative Tools/Capabilities. The creation and implementation of Intellipedia – the IC's version of the user-annotated online encyclopedia Wikipedia, has fostered spontaneous, collaborative analytic efforts, and has enhanced information sharing across the IC on current and emerging issues. Development of additional collaboration tools such as A-Space continues to improve IC information sharing capabilities. The creation of integrated information technology solutions and information sharing applications including consolidated e-mail naming conventions and information capabilities such as iVideo and Intelink further improve information sharing.

We are forging an integrated Intelligence Community that spans the historical divide between foreign and domestic intelligence efforts. Far from being a buzz word, integration means ensuring that our various specialized intelligence missions operate as a single enterprise. An integrated and collaborative Community is a critical advance because no single agency has the capacity to evaluate all available information—lest we forget over one billion pieces of data are collected by America's intelligence agencies everyday.

The principal legacy of the Intelligence Reform Act was the establishment of the Office of the Director of National Intelligence with assigned responsibilities to serve as the chief intelligence advisor to the President and to head the IC to ensure closer coordination and integration. The DNI is afforded responsibility to determine the National Intelligence Program and significant authority over personnel policy. In a larger sense, the creation of the DNI allows one person to see across the wide American Intelligence Community, identify gaps, and promote a strategic, unified direction.

Working closely with the Department of Justice and the FBI, we supported the creation of the FBI's National Security Branch to integrate the FBI's counterterrorism, counterintelligence, WMD, and intelligence programs.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00205 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.013

We established the National Counterterrorism Center (NCTC), the government's hub for all strategic level counterterrorism intelligence assessments, which draws on collected terrorist intelligence from agencies across the U.S. Government with access to more than 30 different networks carrying more than 80 unique data repositories to produce integrated analysis on terrorist plots against U.S. interests at home and abroad.

The results are tangible. NCTC produces a daily threat matrix and situation reports that are the Community standard for current intelligence awareness. In addition, NCTC hosts two video teleconferences daily to discuss the threat matrix and situation reports to ensure the intelligence agencies and organizations see all urgent counterterrorism information.

We also established the National Counterproliferation Center (NCPC), the mission manager for counterproliferation, which has developed integrated and creative strategies against some of the nation's highest priority targets, including "gap attacks" (focused strategies against longstanding intelligence gaps), "over the horizon" studies to address potential future counterproliferation threats, and specialized projects on priority issues such as the Counterterrorism-Counterproliferation Nexus.

The establishment of the Department of Homeland Security (DHS) and DHS's Office of Intelligence and Analysis has enhanced the sharing of information between federal, state, and local government agencies, and the private sector which in turn has enhanced our ability to detect, identify, understand, and assess terrorist threats to and vulnerabilities of the homeland to better protect our Nation's critical infrastructure, integrate our emergency response networks, and link local state and federal governments.

The Terrorist Screening Center was created to consolidate terrorist watch lists and provide around the clock operational support for federal and other government law enforcement personnel across the country.

The growth and maturation of the FBI-led Joint Terrorism Task Forces (JTTF) in major jurisdictions throughout the United States has substantially contributed to improved terrorism-related information sharing and operational capabilities at the state and municipal levels.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00206 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.014

Through these and other efforts, the United States and its coalition partners have made significant strides in defending the homeland against al-Qa'ida, its affiliates, and others who threaten us. Collaboration and information sharing have helped limit the ability of al-Qa'ida and like-minded terrorist groups to operate. We have uncovered and eliminated numerous threats to our citizens and to our friends and allies. We have disrupted terrorist plots, arrested operatives, captured or killed senior leaders, and strengthened the capacity of the Nation to confront and defeat our adversaries.

The Intelligence Community is an adaptive, learning organization. We can and must outthink, outwork, and defeat the enemy's new ideas. Our Intelligence Community is now more collaborative than ever before, knows how to operate as a team, and can adjust to conditions on the ground. We can and will do better, but I cannot guarantee that we can stop all attacks indefinitely. The integrated Intelligence Community as directed in the Intelligence Reform Act is essential; the basic elements of the system are sound; but we must be more flexible and anticipatory.

Fulfilling the goals expressed in the Intelligence Reform and Terrorism Prevention Act, in which this Committee played such a key role, was the right thing for national security in 2004 and is even more critical in 2010; the threats we face demand an integrated intelligence enterprise.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00207 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.015

Statement of Janet A. Napolitano
Secretary

U.S. Department of Homeland Security

before

United States Senate
Committee on Homeland Security and Governmental Affairs

on

Intelligence Reform: The Lessons and Implications of the Christmas Day Attack

Wednesday, January 20, 2010

340 Dirksen Senate Office Building
Washington DC

Chairman Lieberman, Senator Collins, and members of the Committee: Thank you for this opportunity to testify on the attempted terrorist attack on Northwest Flight 253.

The attempted attack on December 25 was a powerful illustration that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. This Administration is determined to thwart those plans and disrupt, dismantle and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just DHS, but many other federal agencies and the international community as well.

As our part in this effort, DHS is a consumer of the U.S. Government's consolidated terrorist watchlist, which we use to help keep potential terrorists off flights within, over or bound for the United States and to identify travelers that require additional screening. We work with foreign governments, Interpol, and air carriers to strengthen global air travel security by advising them on security measures and on which passengers may prove a threat. We also work with air carriers and airport authorities to perform physical screening at TSA checkpoints and to provide security measures in flight.

Immediately following the December 25 attack, DHS took swift action at airports across the country and around the world. These steps included enhancing screening for individuals flying to the United States; increasing the presence of law enforcement and explosives detection canine teams at air ports, and of air marshals in flight; and directing the FAA to notify the 128 flights already inbound from Europe about the situation. Nonetheless, Umar Farouk Abdulmutallab should never have been able to board a U.S.-bound plane with the explosive

56838.017

PETN on his person. As President Obama has made clear, this Administration is determined to find and fix the vulnerabilities in our systems that allowed this breach to occur.

Agencies across the federal government have worked quickly to address what went wrong in the Abdulmutallab case. The effort to solve these problems is well underway, with cooperation among DHS, the Department of State, the Department of Justice, the Intelligence Community, and our international allies, among others. As a consumer of terrorist watchlist information, the Department of Homeland Security welcomes the opportunity to contribute to the dialogue on improving the federal government's ability to connect and assimilate intelligence. We are also focused on improving aviation screening and expanding our international partnerships to guard against a similar type of attack occurring again. To those ends, today I want to describe the role that DHS currently performs in aviation security, how DHS responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

DHS' Role in Multiple Layers of Defense

Since 9/11, the U.S. government has employed multiple layers of defense across several departments to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

DHS oversees several programs to prevent individuals with terrorist ties from boarding flights that are headed to, within, or traveling over the United States or, in appropriate cases, to identify them for additional screening. Specifically, DHS uses information held in the Terrorist Screening Database (TSDB), a resource managed by the Terrorist Screening Center (TSC), as

56838.018

well as other information provided through the Intelligence Community to screen individuals; operates the travel authorization program for people who are traveling to the United States under the Visa Waiver Program (VWP)[1]; and works with foreign governments, international and regional organizations, and airlines to design and implement improved security standards worldwide. This includes routine checks against Interpol databases on wanted persons and lost or stolen passports on all international travelers arriving in the United States. The Department also performs checkpoint screenings at airports in the United States.

To provide a sense of the scale of our operations, every day, U.S. Customs and Border Protection (CBP) processes 1.2 million travelers seeking to enter the United States by land, air or sea; the Transportation Security Administration (TSA) screens 1.8 million travelers at domestic airports; and DHS receives advanced passenger information from carriers operating in 245 international airports that are the last point of departure for flights to the United States, accounting for about 1,600 to 1,800 flights per day. Ensuring that DHS employees and all relevant federal officials are armed with intelligence and information is critical to the success of these efforts.

Safeguards for Visas and Travel

One of the first layers of defense in securing air travel consists of safeguards to prevent dangerous people from obtaining visas, travel authorizations and boarding passes. To apply for entry to the United States prior to boarding flights bound for the U.S. or arriving at a U.S. port of

[1] The 35 countries in the Visa Waiver Program are: Andorra, Australia, Austria, Belgium, Brunei, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, and the United Kingdom (for the U.K., only citizens with an unrestricted right of permanent abode in the U.K. are eligible for VWP travel authorizations).

56838.019

entry, most foreign nationals need visas – issued by a U.S. embassy or consulate – or, if traveling under a Visa Waiver Program country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA) .[2]

Issuing visas is the responsibility of the Department of State. At embassies and consulates where it is operational, the Visa Security Program positions personnel of U.S. Immigration and Customs Enforcement (ICE) to assist State Department personnel in identifying visa applicants who may present a security threat. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. These systems examine an individual's information to assess whether he or she could pose a risk to the United States or its citizens, including possible links to terrorism. Without presenting a valid authorization to travel to the United States at the airport of departure, a foreign national is not able to board a U.S.-bound flight.

The Department also works with other federal agencies and our foreign partners to try to prevent possible terrorists from obtaining boarding passes. These include the application of the No-Fly List and the implementation of Secure Flight program, which I explain below.

Pre-departure screening

As another layer of defense, DHS conducts pre-departure passenger screening in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses TSDB data, managed by the Terrorist Screening Center that is administered by the FBI, to determine who may board, who requires

[2] Exceptions would be citizens of countries under other visa waiver authority such as the Western Hemisphere Travel Initiative or the separate visa waiver program for Guam and the Commonwealth of the Northern Mariana Islands, or those granted individual waivers of the visa requirement under the immigration laws.

56838.020

further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

Through the Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

As an additional layer of security, DHS also uses the Passenger Name Record (PNR), the Advanced Passenger Information System (APIS), and the Immigration Advisory Program (IAP) to assess a passenger's level of risk and, when necessary, flag them for further inspection. PNR data, obtained from the airline reservations systems, contains various elements, which may include optional information on itinerary, co-travelers, changes to the reservation, and payment information. PNR data is evaluated against "targeting rules" that are based on law enforcement data, intelligence and past case experience. APIS data, which carriers are required to provide to

56838.021

DHS at least 30 minutes before a flight, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

Another layer in the screening process is the Immigration Advisory Program (IAP). The CBP officers stationed overseas under the IAP program at nine airports in seven countries receive referrals from CBP screening against the TSDB, of which the No Fly list is a subset. IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Checkpoint screenings and in-flight security

The third layer of defense for air travel in which DHS plays a role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. When a traveler at a foreign airport is physically screened, that screening is conducted by the foreign government, air carriers, or the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the country screen passengers and their baggage using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines,

56838.022

vapor trace machines that detect liquid explosives, Advanced Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers – both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In an effort to enhance international screening standards, TSA conducts security assessments in accordance with security standards established by the International Civil Aviation Organization (ICAO) at more than 300 foreign airports, which include foreign airports from which flights operate directly to the United States and all airports from which U.S. air carriers operate. If an airport does not meet these standards, TSA works with the host government to rectify the deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. In long-term circumstances of non-compliance with international standards, TSA may recommend suspension of flight service from these airports to the United States. In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level. If an airport is located within one of the 35 VWP countries, DHS conducts additional audits and inspections as part of the statutorily mandated VWP designation and review process.

56838.023

In terms of in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers. Additionally, armed law enforcement officers from federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

DHS Response to the Christmas Day Attack

The facts of the Christmas Day attempted bombing are well established and were relayed in the report on the incident that the President released on January 7, 2010. On December 16, 2009, Umar Farouk Abdulmutallab, a Nigerian national, purchased a round-trip ticket from Lagos, Nigeria to Detroit. Abdulmutallab went through physical security screening conducted by foreign airport personnel at Murtala Muhammed International Airport in Lagos on December 24 prior to boarding a flight to Amsterdam Airport Schiphol. This physical screening included an x-ray of his carry-on luggage and his passing through a walk-through metal detector. Abdulmutallab went through additional physical screening, conducted by Dutch authorities, when transiting through Amsterdam to Northwest Flight 253 to Detroit, and presented a valid U.S. visa. Abdulmutallab was not on the No Fly or Selectee Lists. Accordingly, the carrier was not alerted to prevent him from boarding the flight or additional physical screening, nor did the IAP officer advise Dutch authorities of any concerns. As with all passengers traveling on that flight, and similar to all other international flights arriving in the United States, CBP evaluated Abdulmutallab's information while the flight was en route to conduct a preliminary assessment of his admissibility and to determine whether there were requirements for additional inspection.

56838.024

During this assessment, CBP noted that there was a record that had been received from the Department of State, which indicated possible extremist ties. It did not indicate that he had been found to be a threat, or that his visa had been revoked. CBP officers in Detroit were prepared to meet Abdulmutallab upon his arrival for further interview and inspection. The attack on board the flight failed in no small part due to the brave actions of the crew and passengers aboard the plane.

Immediate DHS response

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. That evening, DHS issued a security directive for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

From the first hours following the attempted attack, I worked closely with the President, Assistant to the President for Homeland Security and Counterterrorism John Brennan, senior Department leadership, and agencies across the federal government. I communicated with international partners, members of Congress, state and local leadership and the aviation industry and met with national security experts on counterterrorism and aviation security. The results of

56838.025

these communications culminated in two reports to the President: one on New Year's Eve and the second on January 2, 2010.

One of our most important conclusions was that it is now clearer than ever that air travel security is an international responsibility. Indeed, passengers from 17 countries were aboard Flight 253. Accordingly, DHS has embarked upon an aggressive international program designed to raise international standards for airports and air safety. On January 3, 2010, I dispatched Deputy Secretary Jane Holl Lute and Assistant Secretary for Policy David Heyman to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, they reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists. This afternoon, I am traveling to Spain to meet with my European Union counterparts in the first of a series of global meetings intended to bring about broad consensus on new, stronger, and more consistent international aviation security standards and procedures.

In addition to these efforts, the Department has been in close contact with Congress, our international partners, the aviation industry and state and local officials across the country since the afternoon of the attempted attack. On December 25, the Department issued a joint bulletin with the FBI to state and local law enforcement throughout the nation; conducted calls with major airlines and the Air Transport Association; distributed the FBI-DHS joint bulletin to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country; and notified foreign air carriers with flights to and from the United States of the additional security requirements. DHS has maintained close contact with all of these partners since the attempted attack, and will continue to do so.

56838.026

On January 3, TSA issued a new Security Directive, effective on January 4, which includes long-term, sustainable security measures developed in consultation with law enforcement officials and our domestic and international partners. Because effective aviation security must begin beyond our borders, this Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[3] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners.

Steps Forward to Improve Aviation Security

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. On January 7, I joined Assistant to the President for Counterterrorism and Homeland Security John Brennan to announce five recommendations DHS made to the President as a result of the security reviews ordered by President Obama. At the President's direction, DHS will pursue these five objectives to enhance the protection of air travel from acts of terrorism.

First, DHS will work with our interagency partners to re-evaluate and modify the criteria and process used to create terrorist watchlist, including adjusting the process by which names are added to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them.

[3] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

56838.027

As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, the Department will work closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

Second, DHS will establish a partnership on aviation security with the Department of Energy and its National Laboratories in order to use their expertise to bolster our security. This new partnership will work to develop new and more effective technologies that deter and disrupt known threats, as well as anticipate and protect against new ways that terrorists could seek to board an aircraft with dangerous materials.

Third, DHS will accelerate deployment of Advanced Imaging Technology to provide capabilities to identify materials such as those used in the attempted December 25 attack, and we will encourage foreign aviation security authorities to do the same. TSA currently has 40 machines deployed at nineteen airports throughout the United States, and plans to deploy at least 450 additional units in 2010. DHS will also seek to increase our assets in the area of explosives-trained canines, explosives detection equipment, and other security personnel.

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. As an interim measure, we will deploy law enforcement officers from across DHS to serve as Federal Air Marshals to increase security aboard U.S.-flag carriers' international flights. At the same time, we will maintain the current tempo of operations to support high-risk domestic flights, as we look to longer-term solutions to enhance the training and workforce of the Federal Air Marshal Service.

Fifth, as mentioned earlier, DHS will work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in

56838.028

foreign airports and the commitments of our foreign partners to enhance security – not just for Americans, but also for their nationals traveling to this country.

In all of these action areas to bolster aviation security, we are moving forward with a dedication to safeguard the privacy and rights of travelers.

Conclusion

The attempted attack on Christmas Day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama has made clear that we will be unrelenting in using every element of our national power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities in all sectors. President Obama has clearly communicated the urgency of this task, and the American people rightfully expect swift action. DHS and our federal partners are moving quickly to provide just that.

I wish I could close by giving you a 100 percent guarantee that no terrorist, ever, will try to take down a plane or attack us in some other fashion. I cannot give you such a guarantee; that is not the nature of the world we live in, nor of the threats that we face. What I can give you, however, is the 100 percent commitment of myself, DHS leadership, and the entire DHS enterprise to do everything we can to minimize the risk of terrorist attacks.

Chairman Lieberman, Senator Collins, and members of the Committee: Thank you for this opportunity to testify. I can now answer your questions.

56838.029

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

January 20, 2010

Statement by the Director of National Intelligence
Mr. Dennis C. Blair

My remarks today before the Senate Committee on Homeland Security and Governmental Affairs have been misconstrued. The FBI interrogated Umar Farouk Abdulmutallab when they took him into custody. They received important intelligence at that time, drawing on the FBI's expertise in interrogation that will be available in the HIG once it is fully operational.

# # #

56838.377

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INSTRUCTION NO. 80.05

Category 80 – Information Management
Office of Primary Responsibility: Civil Liberties and Privacy Office

SUBJECT: IMPLEMENTATION OF PRIVACY GUIDELINES FOR SHARING PROTECTED INFORMATION

1. AUTHORITIES: National Security Act of 1947, as amended; Executive Order 13388; Executive Order 12333, as amended; Privacy Act of 1974, as amended; Presidential Memorandum dated December 16, 2005 (*Guidelines and Requirements in Support of the Information Sharing Environment*); and other applicable provisions of law.

2. REFERENCES: ODNI Instruction No. 2006-3, *Protection of Privacy and Civil Liberties*; ODNI Instruction 80.02, *Managing Breaches of Personally Identifiable Information*; *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (the Guidelines, see attached); Intelligence Community Directive 102 *Process for Developing Interpretive Principles and Proposing Amendments to Attorney General Guidelines Governing the Collection, Retention, and Dissemination of Information Regarding U.S. Persons*; and the *Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment and Privacy and Civil Liberties Implementation Workbook for Federal Agencies* provided at www.ise.gov.

3. PURPOSE: This Instruction governs how the Office of the Director of National Intelligence (ODNI) handles records containing information about protected individuals (i.e., "protected information") when those records are disclosed to or received from other federal agencies; state, local, tribal, and foreign terrorism information sharing partners; and the private sector. Processes outlined in this Instruction will assist the ODNI in complying with applicable privacy and civil liberties requirements with respect to sharing protected information, and with the safeguards for United States citizens and permanent resident aliens embodied in Executive Order (EO) 12333, and in guidelines and procedures implementing the provisions and protections of EO 12333.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00223 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.030

4. APPLICABILITY: This Instruction applies to all ODNI staff, detailees, assignees, contractors, and others who have access to ODNI information or systems that may be used in the sharing of terrorism-related information containing information about protected individuals.

5. DEFINITIONS: The following definitions apply to this Instruction:

A. Information Sharing Environment (ISE): The ISE is an approach for sharing "protected information" contained in terrorism-related information (including information on weapons of mass destruction, homeland security information, and law enforcement information related to terrorism) with federal, state, local, tribal, and private sector entities, as well as foreign partners. Mandated by Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the ISE is composed of the policies, processes, protocols, and technologies that govern the handling and management of "protected information" subject to exchange with other entities. In practical effect, the term "ISE" refers to procedures for the sharing of terrorism information that contains information about protected individuals.

B. Protected Information: Protected information is information about United States citizens and permanent resident aliens that is subject to information privacy or other legal protections under the U.S. Constitution and federal laws. Protected information may also include information designated by Executive Order, international agreement or other instrument as subject to information privacy or other protections.

6. POLICY: All persons identified in Paragraph 4 shall ensure that information privacy, civil liberties, and other legal rights of American citizens and permanent resident aliens are protected as terrorism-related information is exchanged between information sharing partners.

7. ROLES AND RESPONSIBILITIES:

A. The ODNI Civil Liberties Protection Officer (CLPO) is hereby designated the ODNI ISE Privacy Officer. In consultation with other responsible ODNI offices, the CLPO shall:

(1) Oversee the ODNI's implementation of and compliance with the Guidelines;

(2) Ensure that policies, procedures, and systems comply with the Guidelines;

(3) Design, implement, and manage privacy and civil liberties training;

(4) Provide guidance for implementing this Instruction;

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00224 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.031

(5) Review and assess complaints in accordance with Paragraph 13 of this Instruction.

B. All ODNI components shall:

(1) Consult with the CLPO to determine the need to formalize a Standard Operating Procedure (SOP), which may be issued as an Internal Process Document (IPD), for implementing this Instruction. If an SOP is necessary, the component shall designate a senior official responsible for developing and implementing the SOP.

(2) Consult with the CLPO, when no SOP is needed, to ensure compliance with this Instruction.

(3) Ensure that protected information meets the standards of accuracy, completeness, and consistency described in Paragraph 10 below.

C. The Data Integrity and ISE Oversight Board shall evaluate components' processes and identify additional protections needed as described in Paragraph 12.B. below.

8. PROCESS TO ENSURE COMPLIANCE WITH LAWS:

A. Components seeking to share protected information with ODNI's terrorism information sharing partners shall ensure that the protected information is subject to a thorough review of the privacy, civil liberties, EO 12333 guidelines, and other applicable conditions and requirements for sharing ("ISE rules review," or "rules review"). Subject to further CLPO guidance, components shall:

(1) Consult with CLPO and other offices as CLPO may designate, (e.g., Office of the General Counsel, Mission Support Center/Information Management), document such consultations, and receive written affirmation from reviewing or consulting officials or offices that appropriate criteria have been met; **OR**

(2) Prescribe an internal ISE rules review process as part of an SOP developed pursuant to Section 7(b) of this Instruction and that meets with CLPO approval; **AND**

(3) Document all data sharing between the ODNI and other entities via terms of reference, Attorney General Guidelines, Memoranda of Understanding (MOU) or similar instruments, and ensure review and approval of such documentation by the CLPO and other offices the CLPO may designate.

B. In conducting the rules reviews, CLPO, the Office of the General Counsel (OGC), and other relevant offices shall work with components to:

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00225 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.032

(1) Identify privacy, civil liberties, EO 12333, and other requirements that apply to the protected information to be shared;

(2) Develop an IPD identifying any rules specific to particular sharing arrangements or categories of protected information; and

(3) Establish safeguards to ensure that:

(a) Protected information is not shared solely on the basis of the exercise of rights guaranteed by the First Amendment, or on the basis of race, ethnicity, national origin, or religious affiliation; and

(b) Controls and limitations are implemented for protected information as applicable law or policy requires.

C. If, in conducting rules reviews, the CLPO, OGC, or any ODNI component identifies:

(1) An issue that erodes information privacy rights, civil liberties, U.S. person or other legal protections, the CLPO, upon identifying or receiving notice of such issue, shall initiate any internal reviews and policy processes needed to address the risk to protected rights or information;

(2) An internally imposed restriction on sharing protected information that impedes the sharing of terrorism, homeland security, or law enforcement information and that does not appear to be required by applicable laws or to protect information privacy, civil liberties, or other legal rights, the CLPO, upon identifying or receiving notice of such restriction, shall initiate any internal reviews and policy processes needed to address the apparent impediment; or

(3) A restriction of the type described in the above paragraph that is imposed by a requirement external to ODNI, the CLPO, and OGC shall review such reported impediments, consult with the ISE Privacy Guidelines Committee, and, failing internal resolution of the concern, bring such restriction to the attention of the Attorney General and the Director of National Intelligence pursuant to the ISE Privacy Guidelines.

9. CHARACTER OF DATA - NOTICE:

A. Components will provide a cover sheet or electronic banner, legend or screen notifying recipient agencies of the nature of the records, data, databases or systems of records, and appropriate approved control markings for unclassified information which they make available to other terrorism-related information sharing partners. The notice shall state whether the information:

(1) Contains protected information pertaining to a United States citizen or permanent resident alien, or a non-immigrant alien protected by treaty or international agreement;

(2) Is subject to legal restrictions on its access, use, or disclosure, and describes the restriction and pertinent law, regulation or policy; or,

(3) Is generally reliable and accurate. If its reliability and accuracy is unknown, describe the reason for limited confidence in source reliability or content validity (e.g., notice from previous recipient of data, independent review, or inconsistency in records).

B. Components shall also use the cover sheet or electronic banner, legend or screen to provide to the recipient agency POC pertinent contact information for the terrorism-related reports, records or data they disseminate. At a minimum, this information should include the name of the originating department or activity, and, if possible, the title and contact data for the person to whom questions regarding the information should be directed.

10. DATA QUALITY: The standards outlined below are the minimum required; components may impose stricter data quality standards.

A. Data Quality Reviews: Components shall ensure that protected information meets the standards of accuracy, completeness, and consistency required to further the purpose(s) for which the information is collected and used. Specifically:

(1) To prevent, identify, and correct errors, components shall conduct and document quality assurance reviews of protected data to the extent feasible, notwithstanding exemption from review under the Privacy Act of 1974 or other law;

(2) Components may document the decision that a data quality review conducted to satisfy a non-ISE legal or policy requirement (e.g., OMB mandate, term of MOU) is current and appropriate for the data set examined, recording date of review, and legal authority/requirement for review;

(3) Components shall document a decision to review data sets in stages, based on priority areas or criticality of accuracy;

(4) Reviews may include comparison of records to detect inconsistencies or other concerns about accuracy.

B. Data Quality Processes: Components shall articulate processes and criteria to ensure:

(1) Merged/matched records relate to the same individual;

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00227 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.034

(2) Errors, inconsistencies, and deficiencies are investigated and corrected/deleted in a timely manner;

(3) Outdated or irrelevant data is updated, deleted or segregated in a timely manner; and

(4) Data that is pending correction, updating, or deletion is withheld from disclosure or access or is appropriately segregated.

C. Notice of Errors in Data Received: When a component determines that protected information originating from an external source may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the protected individual may be affected:

(1) The potential error or deficiency shall be communicated in writing to the ODNI CLPO, as well as to the other agency's ISE Privacy/Civil Liberties Official (identified in the applicable MOU or other instrument governing the information exchange); and

(2) The communication shall include information that clarifies, limits, contradicts or qualifies the information deemed to be erroneous or deficient.

D. Notice of Errors in Data Disseminated: When a component determines that protected information it originated is or may be erroneous or non-compliant with terrorism-related information sharing policy or other policy or statute, and knows or believes (based on logs/audit) that the information was accessed by another agency, the component shall take the following steps:

(1) Provide written notice to the ODNI CLPO of the deficiency, assessing the extent to which the protected information has been disseminated;

(2) Notify record recipients of the deficiency, if they can be identified, to include information that clarifies, contradicts or qualifies the deficient information;

(3) Correct or delete the erroneous information, or follow appropriate processes to dispose of the record. When it is uncertain whether the protected information is erroneous, note known limitations on accuracy in the field containing the protected information.

(4) Report the erroneous dissemination to the Intelligence Oversight Board and to the Director of National Intelligence (DNI) as appropriate pursuant to Executive Order 12333.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00228 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.035

E. Notice of Data Erroneously Shared: A component that shares protected information erroneously or in a manner that is inconsistent with this Instruction shall immediately:

(1) Recall the information by contacting all record recipients of the information and request immediate destruction of all disseminated copies of the information;

(2) Comply with Instruction 80.02, *Managing Breaches of Personally Identifiable Information*, and report the matter to the CLPO, who shall convene an Incident Response Team to evaluate the disclosure, decide if notice to record subjects is required, and, as needed, develop a response plan.

F. Data Integrity and ISE Oversight Board: As described in Section 12.B. below, the Board will assess overall data quality and respond to identified data quality issues.

11. DATA SECURITY: An ODNI component sharing protected information through the ISE shall:

A. Obtain assurances from the Mission Support Center (MSC) that MSC offices have implemented policies prescribing administrative, technical, and physical safeguards for protected information or will implement them soon. MSC policies should reflect, as applicable, the standards and directives in the Data Security sections of the *Privacy and Civil Liberties Implementation Workbook for Federal Agencies*.

B. Coordinate with the ODNI/Chief Information Officer to implement appropriate privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

12. ACCOUNTABILITY, ENFORCEMENT, AND AUDITABILITY:

A. Components are responsible for cooperating with all ISE protected information audits and reviews conducted as set forward in Sections 12.B and 12.C. All completed reviews and audits shall be submitted to the CLPO.

B. ODNI CLPO shall establish a "Data Integrity and Oversight Board (Board)" with representation from each ODNI component that shares information through the ISE. The Board also shall include a representative from the IMO. The Board will oversee components' rules review and terrorism data inventory processes; examine data quality reviews to identify potential problem areas; and identify processes, policies or training to minimize the use or dissemination of erroneously protected information and to ensure that technical protections are implemented.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00229 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.036

C. The ODNI CLPO shall work with components to implement audit procedures relating to the sharing of protected information with terrorism-related information sharing partners. Audits may be conducted on any or all of the elements addressed by the Privacy Guidelines.

13. REDRESS:

A. General: Components receiving requests for access to protected information, or complaints from individuals who believe protected information about them has been shared, shall identify the appropriate office through which to seek redress.

B. Requests for Access to ODNI Information: Responses to requests from individuals seeking access to protected information about them that is under an ODNI Component's control shall be addressed as prescribed by ODNI Instruction 80.01, *Freedom of Information Act and Privacy Act Program* and corresponding Privacy Act Regulations (32 CFR Part 1701). Such requests shall be forwarded to the ODNI Information Management Officer, who will maintain a file of such requests and take action as appropriate.

C. Information Sharing Complaints, CLPO Role, and ODNI Component Support:

(1) A component or ODNI redress action office that receives a complaint or allegation relating to the sharing of protected information shall promptly forward the complaint or allegation to the ODNI CLPO for acknowledgement, investigation, and resolution, as appropriate.

(2) CLPO shall be responsible for handling complaints or requests for redress involving terrorism-related information which is not identifiable as within the authority or responsibility of any of the other ODNI-internal offices.

(3) CLPO shall reconcile protocols for handling complaints arising, variously, under privacy and civil liberties authorities and under EO 12333, and components shall cooperate with procedures developed for conducting internal and external investigations and for communicating with complainants regarding the handling of all protected information.

D. Expungement: Components receiving expungement orders issued by a federal court shall forward them to the OGC, with a copy to CLPO and MSC/IM. Components will coordinate with the OGC and IMO to comply with expungement orders and to determine how to respond to expungement orders issued by state courts.

E. Interagency Cooperation: Subject to ODNI authorities, ODNI will respond as promptly as practicable to a request for information and cooperation from another agency to assist in addressing a complaint received by such other agency. ODNI, conversely,

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00230 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.037

shall promptly request the assistance of other information sharing partners when a request is received that relates to the activities of the other partner in respect to terrorism-related information.

14. TRAINING: Privacy, civil liberties, and U.S. person training will be mandatory for all personnel who collect, have access to, or disseminate protected information. The ODNI CLPO is responsible for designing, implementing, and managing this training.

A. The training program will, at a minimum, cover the following topics:

(1) Collection, retention, use, and dissemination of protected information;

(2) Reporting violations of privacy-protection policies; and,

(3) Sanctions for misuse of protected data and non-compliance with Guidelines.

B. ODNI personnel who have access to protected information, or operate/maintain databases or National Security Systems, shall certify their participation in annual ODNI privacy, civil liberties, and U.S. person training.

C. ODNI will provide training to ensure that all agency action offices possessing a redress function are familiar with ODNI's terrorism-related information sharing activities, and understand when a complaint or inquiry received implicates protected information subject to action by CLPO.

15. INTERNAL AWARENESS: The ODNI CLPO will facilitate appropriate internal awareness of its policies and procedures for implementing the Guidelines. This Instruction shall be available on the ODNI classified website. The CLPO shall ensure that information about privacy, civil liberties, and EO 12333 policies and procedures is updated as necessary.

16. NON-FEDERAL ENTITIES: To the extent consistent with applicable laws and guidance, the ODNI will share, as appropriate, terrorism, homeland security, and/or law enforcement information related to terrorism with state, local, and tribal governments, law enforcement agencies, and non-government entities provided they implement privacy protections that are at least as comprehensive as those prescribed by the ISE Guidelines. The Program Manager-Information Sharing Environment (PM-ISE) shall provide guidance on the privacy and civil liberties protection policies that non-federal entities should adopt in order to receive terrorism, homeland security and/or law enforcement information related to terrorism from federal terrorism information sharing partners.

A. The National Counterterrorism Center will facilitate the production of "federally coordinated" terrorism-related information for use by state, local, and tribal governments, law enforcement agencies, and non-government entities.

B. Components shall consult with the CLPO and Policies, Plans and Requirements (PPR) in anticipation of sharing terrorism information with non-federal entities.

17. EFFECTIVE DATE: This Instruction is effective upon signature.

John F. Kimmons

2 Sep 09

John F. Kimmons
Lieutenant General, USA
Director of the Intelligence Staff

Date

Attachment: *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment*

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00232 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.039

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment

1. Background and Applicability.

a. *Background.* Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, "[t]o the maximum extent consistent with applicable law, agencies shall ... give the highest priority to ... the interchange of terrorism information among agencies ... [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities ...." These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.

b. *Applicability.* These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

2. Compliance with Laws.

a. *General.* In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.

b. *Rules Assessment.* Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00233 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.040

(i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

(ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

c. *Changes.* If, as part of its rules assessment process, an agency:

(i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue;

(ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;

(iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

3. Purpose Specification.

Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00234 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.041

information available through the ISE is consistent with the authorized purpose of the ISE.

4. Identification of Protected Information to be Shared through the ISE.

a. *Identification and Prior Review.* In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.

b. *Notice Mechanisms.* Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

(i) the information pertains to a United States citizen or lawful permanent resident;

(ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and

(iii) there are limitations on the reliability or accuracy of the information.

5. Data Quality.

a. *Accuracy.* Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

b. *Notice of Errors.* Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00235 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.042

the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).

c. *Procedures.* Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

(i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;

(ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and

(iii) retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

6. Data Security.

Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction

7. Accountability, Enforcement and Audit.

a. *Procedures.* Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:

(i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;

(ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;

(iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00236 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.043

(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. Audit. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

8. Redress.

To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

9. Execution, Training, and Technology.

a. Execution. The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.

b. Training. Each agency shall develop an ongoing training program in the implementation of these Guidelines, and shall provide such training to agency personnel participating in the development and use of the ISE.

c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

10. Awareness.

Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

11. Non-Federal Entities.

Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work with non-Federal entities seeking to access protected information through the ISE to ensure that such non-Federal entities

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00237 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.044

develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

12. Governance.

a. *ISE Privacy Officials.* Each agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.

b. *ISE Privacy Guidelines Committee.* All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide ongoing guidance on the implementation of these Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, executive order, or as part of the ISE, and will as appropriate work through or in consultation with such other mechanisms. The ISE Privacy Guidelines Committee shall be chaired by the PM or a senior official designated by the PM, and will consist of the ISE privacy officials of each member of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee, the PM will address the issue through the established ISE governance process. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE governance process evolves, if a different entity is established or

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00238 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.045

identified that could more effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.

c. *Privacy and Civil Liberties Oversight Board.* The Privacy and Civil Liberties Oversight Board (PCLOB) should be consulted for ongoing advice regarding the protection of privacy and civil liberties in agencies' development and use of the ISE. To facilitate the performance of the PCLOB's duties, the ISE Privacy Guidelines Committee will serve as a mechanism for the PCLOB to obtain information from agencies and to provide advice and guidance consistent with the PCLOB's statutory responsibilities. Accordingly, the ISE Privacy Guidelines Committee should work in consultation with the PCLOB, whose members may attend Committee meetings, provide advice, and review and comment on guidance as appropriate.

d. *ISE Privacy Protection Policy.* Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines. Agencies should consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.

13. General Provisions.

a. Definitions.

(i) The term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office.

(ii) The term "protected information" has the meaning set forth for such term in paragraph 1(b) of these Guidelines.

(iii) The terms "terrorism information," "homeland security information," and "law enforcement information" are defined as follows:

"Terrorism information," consistent with section 1016(a)(4) of IRTPA means all relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00239 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.046

domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, (C) communications of or by such groups or individuals, or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

"Homeland security information," as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal, State, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or (D) a planned or actual response to a terrorist act.

"Law enforcement information" for the purposes of the ISE means any information obtained by or of interest to a law enforcement agency or official that is (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

b. The treatment of information as "protected information" under these Guidelines does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.

c. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00240 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.047

d. These Guidelines:

(i) shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

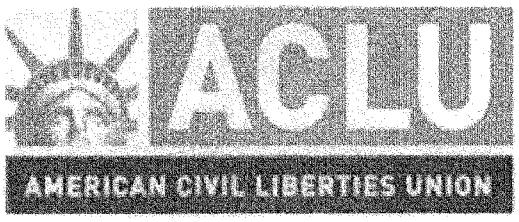
(ii) shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

(iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(iv) are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00241 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.048



Written Statement of the

American Civil Liberties Union

Michael W. Macleod-Ball

Acting Director, Washington Legislative Office

Christopher Calabrese

Legislative Counsel

before the

Senate Committee on Homeland Security

& Governmental Affairs

January 20, 2009

Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part I

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00242 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.049

WASHINGTON LEGISLATIVE OFFICE

915 15th Street, NW Washington, D.C. 20005

(202) 544-1681 Fax (202) 546-0738

Written Statement of the

American Civil Liberties Union

Michael W. Macleod-Ball

Acting Director, Washington Legislative Office

Christopher Calabrese

Legislative Counsel

before the

Senate Committee on Homeland Security & Governmental Affairs

January 20, 2010

Chairman Lieberman, Ranking Member Collins, and Members of the Committee:

The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. In particular, throughout our history, we have been one of the nation's pre-eminent advocates in support of privacy and equality. We write today to express our strong concern over the three substantive policy changes that are being considered in the wake of the attempted terror attack on Christmas Day: the wider deployment of whole body imaging (WBI) devices, the expanded use of terror watch lists and increased screening of individuals from fourteen so-called nations of interest. The ACLU believes that each of these technologies greatly infringe on civil liberties and face serious questions regarding its efficacy in protecting airline travelers.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00243 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.050

The President has already identified a failure of intelligence as the chief cause of the inability to detect the attempted terror attack on Christmas day. As such, the government's response must be directed to that end. These invasive and unjust airline security techniques represent a dangerous diversion of resources from the real problem. This diversion of resources promises serious harm to American's privacy and civil liberties while failing to deliver significant safety improvements.

I. Introduction

WBI uses millimeter wave or X-ray technology to produce graphic images of passengers' bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. This technology is currently deployed at 19 airports and the Department of Homeland Security (DHS) recently announced the roll out of 300 more machines by year end. [1] While initially described as a secondary screening mechanism, DHS is now stating that WBI will be used for primary screening of passengers.[2]

Another way of screening passengers is through terror watch lists. The terror watch lists are a series of lists of names of individuals suspected of planning or executing terrorist attacks. The master list is maintained by the Terrorist Screening Center (TSC) and contains more than one million names.[3] Subsets of this list include the No Fly list (barring individuals from air travel) and the Automatic Selectee list (requiring a secondary screening). The names on this list and the criteria for placement on these lists are secret.[4] There is no process allowing individuals to challenge their placement on a list or seek removal from a list.

Finally, individuals who were born in, are citizens of, or are traveling from fourteen nations will receive additional scrutiny under a policy announced by the US government after the attempted terror attack. As of January 19, 2010 these nations are Afghanistan, Algeria, Cuba, Iran, Lebanon, Libya, Iraq, Nigeria, Pakistan, Saudi Arabia, Somalia, Sudan, Syria and Yemen.

The ACLU believes that Congress should apply the following two principles in evaluating any airline security measure:

- **Efficacy.** New security technologies must be genuinely effective, rather than creating a false sense of security. The wisdom supporting this principle is obvious: funds to increase aviation security are limited, and any technique or technology must work and be substantially better than other alternatives to deserve some of the limited funds available. It therefore follows that before Congress invests in technologies or employs new screening methods, it must

---

[1] Harriet Baskas, *Air security: Protection at privacy's expense?* Msnbc.com, January 14, 2010. http://www.msnbc.msn.com/id/34846903/ns/travel-tips/

[2] Paul Giblin and Eric Lipton, *New Airport X-Rays Scan Bodies, Not Just Bags*, New York Times, February 24, 2007.

[3] *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Justice Department, Office of the Inspector General, Audit Report 09-25, May 2009, pg 3. http://www.justice.gov/oig/reports/FBI/a0925/final.pdf

[4] *Id* at 70.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00244 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.051

demand evidence and testing from neutral parties that these techniques have a likelihood of success.

- **Impact on Civil Liberties.** The degree to which a proposed measure invades privacy should be weighed in the evaluation of any technology. If there are multiple effective techniques for safeguarding air travel, the least intrusive technology or technique should always trump the more invasive technology.

II. Screening Techniques and Technologies Must Be Effective, or they Should Not be Utilized or Funded

The wider deployment of whole body imaging (WBI) devices, expanded use of terror watch lists and increased screening of individuals from fourteen so-called nations of interest each face significant questions regarding their efficacy in protecting air travelers and combating terrorism.

Whole Body Imaging

There are no magic solutions or technologies for protecting air travelers. Ben Wallace, a current member of the British parliament who advised a research team at *QinetiQ*, a manufacturer of body screening devices, has stated that their testing demonstrated that these screening devices would not have discovered a bomb of the type used on Christmas day, as they failed to detect low density materials like powders, liquids and thin plastics. [5] A current QinetiQ product manager admitted that even their newest body scan technology probably would not have detected the underwear bomb.[6] The British press has also reported that the British Department for Transport (DfT) and the British Home Office have already tested the scanners and were not convinced they would work comprehensively against terrorist threats to aviation.[7]

In addition we know that al Qaeda has already discovered a way to work around this technology. In September a suicide bomber stowed a full pound of high explosives and a detonator inside his rectum, and attempted to assassinate a Saudi prince by blowing himself up.[8] While the attack only slightly wounded the prince, it fully defeated an array of security measures including metal detectors and palace security. The bomber spent 30 hours in the close company of the prince's own secret service agents – all without anyone suspecting a thing. WBI devices – which do not penetrate the body – would not have detected this device.

The practical obstacles to effective deployment of body scanners are also considerable. In the United States alone, 43,000 TSA officers staff numerous security gates at over 450 airports and over 2 million passengers a day.[9] To avoid being an ineffective "Maginot line," these $170,000 machines will need to be put in place at all gates in all airports; otherwise a

[5] Jane Merrick, *Are planned airport scanners just a scam?* The Independent, January 3, 2010.
[6] *Id.*
[7] *Id.*
[8] Sheila MacVicar , *Al Qaeda Bombers Learn from Drug Smugglers*, CBSnews.com, September 28, 2009
[9] http://www.tsa.gov/what_we_do/screening/security_checkpoints.shtm

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00245 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.052

terrorist could just use an airport gate that does not have them. Scanner operators struggle constantly with boredom and inattention when tasked with the monotonous job of scanning thousands of harmless individuals when day after day, year after year, no terrorists come through their gate. In addition to the expense of buying, installing and maintaining these machines, additional personnel will have to be hired to run them (unless they are shifted from other security functions, which will degrade those functions).

The efficacy of WBI devices must be weighed against not only their impact on civil liberties (discussed further below) but also their impact on the U.S. ability to implement other security measures. Every dollar spent on these technologies is a dollar that is not spent on intelligence analysis or other law enforcement activity. The President has already acknowledged that it was deficiencies in those areas – not aviation screening – that allowed Umar Farouk Abdulmutallab to board an airplane.

Watch Lists

The events leading up to the attempted Christmas attack are a telling indictment of the entire watch list system. In spite of damning information, including the direct plea of Abdulmutallab's father, and other intelligence gathered about terrorist activity in Yemen, Abdulmutallab was not placed into the main Terrorist Screening Database. We believe that fact can be directly attributed to the bloated and overbroad nature of the list – now at more than a million names.[10] The size of the list creates numerous false positives, wastes resources and hides the real threats to aviation security. As we discuss below it also sweeps up many innocent Americans – falsely labeling them terrorists and providing them with no mechanism for removing themselves from the list.

These problems are not hypothetical. They have real consequences for law enforcement and safety. An April 2009 report from the Virginia Fusion Center states

> According to 2008 Terrorism Screening Center ground encounter data, al-Qa'ida was one of the three most frequently encountered groups in Virginia. In 2007, at least 414 encounters between suspected al-Qa'ida members and law enforcement or government officials were documented in the Commonwealth. Although the vast majority of encounters involved automatic database checks for air travel, a number of subjects were encountered by law enforcement officers.[11]

Every time a law enforcement officer encounters someone on the terrorist watch list (as determined by a check of the National Crime Information Center (NCIC) database) they contact the TSC. So in essence Virginia law enforcement is reporting that there are more than 400 al Qaeda terrorists in Virginia in a given year. This is difficult to believe. [12] In reality most, if not all, of these stops are false positives, mistakes regarding individuals who should not be on the list. These false positives can only distract law enforcement from real dangers.

---

[10] *DOJ OIG* Audit Report 09-25, pg 3. http://www.justice.gov/oig/reports/FBI/a0925/final.pdf
[11] Virginia Fusion Center, *2009 Virginia Terrorism Threat Assessment*, March 2009, pg 27.
[12] The report does not state that any of these individuals were arrested.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00246 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.053

A 2009 report by the Department of Justice Inspector General found similarly troubling results. From the summary:

> We found that the FBI failed to nominate many subjects in the terrorism investigations that we sampled, did not nominate many others in a timely fashion, and did not update or remove watchlist records as required. Specifically, in 32 of the 216 (15 percent) terrorism investigations we reviewed, 35 subjects of these investigations were not nominated to the consolidated terrorist watchlist, contrary to FBI policy. We also found that 78 percent of the initial watchlist nominations we reviewed were not processed in established FBI timeframes.
>
> Additionally, in 67 percent of the cases that we reviewed in which a watchlist record modification was necessary, we determined that the FBI case agent primarily assigned to the case failed to modify the watchlist record when new identifying information was obtained during the course of the investigation, as required by FBI policy. Further, in 8 percent of the closed cases we reviewed, we found that the FBI failed to remove subjects from the watchlist as required by FBI policy. Finally, in 72 percent of the closed cases reviewed, the FBI failed to remove the subject in a timely manner.[13]

This is only the latest in a long string of government reports describing the failure of the terror watch lists.[14] In order to be an effective tool against terrorism these lists must shrink dramatically with names limited to only those for whom there is credible evidence of terrorist ties or activities.

Aviation Screening on the Basis of Nationality

Numerous security experts have already decried the use of race and national origin as an aviation screening technique.

Noted security expert Bruce Schneier stated recently:

> [A]utomatic profiling based on name, nationality, method of ticket purchase, and so on...makes us all less safe. The problem with automatic profiling is that it doesn't work.

---

[13] *DOJ OIG* Audit Report 09-25, pg iv-v. http://www.justice.gov/oig/reports/FBI/a0925/final.pdf

[14] *Review of the Terrorist Screening Center (Redacted for Public Release)*, Justice Department, Office of the Inspector General, Audit Report 05-27, June 2005; *Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program (Redacted for Public Release)*, Justice Department, Office of the Inspector General, Audit Report 05-34, August 2005; *Follow-Up Audit of the Terrorist Screening Center (Redacted for Public Release)*, Justice Department, Office of the Inspector General, Audit Report 07-41, September 2007; *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Justice Department, Office of the Inspector General, Audit Report 09-25, May 2009; *DHS Challenges in Consolidating Terrorist Watch List Information*, Department of Homeland Security, Office of Inspector General, OIG-04-31, August 2004; *Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO Report to Congressional Requesters, GAO-03-322, April 2003; *Congressional Memo Regarding Technical Flaws in the Terrorist Watch List*, House Committee on Science and Technology, August 2008.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00247 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.054

Terrorists can figure out how to beat any profiling system.

Terrorists don't fit a profile and cannot be plucked out of crowds by computers. They're European, Asian, African, Hispanic, and Middle Eastern, male and female, young and old. Umar Farouk Abdul Mutallab was Nigerian. Richard Reid, the shoe bomber, was British with a Jamaican father. Germaine Lindsay, one of the 7/7 London bombers, was Afro-Caribbean. Dirty bomb suspect Jose Padilla was Hispanic-American. The 2002 Bali terrorists were Indonesian. Timothy McVeigh was a white American. So was the Unabomber. The Chechen terrorists who blew up two Russian planes in 2004 were female. Palestinian terrorists routinely recruit "clean" suicide bombers, and have used unsuspecting Westerners as bomb carriers.

Without an accurate profile, the system can be statistically demonstrated to be no more effective than random screening.

And, even worse, profiling creates two paths through security: one with less scrutiny and one with more. And once you do that, you invite the terrorists to take the path with less scrutiny. That is, a terrorist group can safely probe any profiling system and figure out how to beat the profile. And once they do, they're going to get through airport security with the minimum level of screening every time.[15]

Schneier is not alone in this assessment. Philip Baum is the managing director of an aviation security company:

Effective profiling is based on the analysis of the appearance and behavior of a passenger and an inspection of the traveler's itinerary and passport; it does not and should not be based on race, religion, nationality or color of skin. ...

Equally, the decision to focus on nationals of certain countries is flawed and backward. Perhaps I, as a British citizen, should be screened more intensely given that Richard Reid (a.k.a "the Shoebomber") was a U.K. passport holder and my guess is there are plenty more radicalized Muslims carrying similar passports. Has America forgotten the likes of Timothy McVeigh? It only takes one bad egg and they exist in every country of the world. [16]

Former Israeli airport security director Rafi Ron:

My experience at Ben Gurion Airport in Tel Aviv has led me to the conclusion that racial profiling is not effective. The major attacks at Ben Gurion Airport were carried out by Japanese terrorists in 1972 and Germans in the 1980s. [They] did not belong to

[15] http://roomfordebate.blogs.nytimes.com/2010/01/04/will-profiling-make-a-difference/
[16] *Id.*

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00248 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.055

any expected ethnic group. Richard Reid [known as the shoe bomber] did not fit a racial profile. Professionally as well as legally, I oppose the idea of racial profiling.[17]

This should be the end of the discussions. Policies that don't work have no place in aviation security. When they are actively harmful – wasting resources and making us less safe – they should be stopped as quickly as possible.

III. The Impact on Privacy and Civil Liberties Must be Weighed in Any Assessment of Aviation Security Techniques

Each of the three aviation security provisions discussed in these remarks represents a direct attack on fundamental American values. As such they raise serious civil liberties concerns.

Whole Body Imaging

WBI technology involves a striking and direct invasion of privacy. It produces strikingly graphic images of passengers' bodies, essentially taking a naked picture of air passengers as they pass through security checkpoints. It is a virtual strip search that reveals not only our private body parts, but also intimate medical details like colostomy bags. Many people who wear adult diapers feel they will be humiliated. That degree of examination amounts to a significant assault on the essential dignity of passengers. Some people do not mind being viewed naked but many do and they have a right to have their integrity honored.

This technology should not be used as part of a routine screening procedure, but only when the facts and circumstances suggest that it is the most effective method for a particular individual. And such technology may be used in place of an intrusive search, such as a strip search – when there is reasonable suspicion sufficient to support such a search.

TSA is also touting privacy safeguards including blurring of faces, the non-retention of images, and the viewing of images only by screeners in a separate room. Scanners with such protections are certainly better than those without; however, we are still skeptical of their suggested safeguards such as obscuring faces and not retaining images.

Obscuring faces is just a software fix that can be undone as easily as it is applied. And obscuring faces does not hide the fact that rest of the body will be vividly displayed. A policy of not retaining images is a protection that would certainly be a vital step for such a potentially invasive system, but it is hard to see how this would be achieved in practice. TSA would almost certainly have to create exceptions – for collecting evidence of a crime or for evaluation of the system (such as in the event of another attack) for example – and it is a short step from there to these images appearing on the Internet.

---

[17] Katherine Walsh, *Behavior Pattern Recognition and Why Racial Profiling Doesn't Work*, CSO Online, (Feb. 1, 2006), at: http://www.csoonline.com/article/220787/Behavior_Pattern_Recognition_and_Why_Racial_Profiling_Doesn_t_Work

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00249 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.056

Intrusive technologies are often introduced very gingerly with all manner of safeguards and protections, but once the technology is accepted the protections are stripped away. There are substantial reasons for skepticism regarding TSA promised protections for WBI devices. In order for these protections to be credible Congress must enshrine them in law.

Finally, the TSA should invest in developing other detection systems that are less invasive, less costly and less damaging to privacy. For example, "trace portal detection" particle detectors hold the promise of detecting explosives while posing little challenge to flyers' privacy. A 2002 Homeland Security report urged the "immediate deployment" of relatively inexpensive explosive trace detectors in European airports, as did a 2005 report to Congress, yet according to a 2006 Associated Press article, these efforts "were frustrated inside Homeland Security by 'bureaucratic games, a lack of strategic goals and months-long delays in distributing money Congress had already approved."[18] Bureaucratic delay and mismanagement should not be allowed to thwart the development of more effective explosive detection technologies that do not have the negative privacy impact of WBI devices.

Watch Lists

The creation of terrorist watch lists – literally labeling individuals as a terrorist – has enormous civil liberties impact. It means ongoing and repetitive harassment at all airports – foreign and domestic, constant extra screening, searches and invasive questions. For the many innocent individuals on the lists this is humiliating and infuriating.

For some it is worse. Individuals on the no fly list are denied a fundamental right, the right to travel and move about the country freely. Others are threatened with the loss of their job. Erich Sherfen, commercial airline pilot and Gulf War veteran, has been threatened with termination from his job as a pilot because his name appears on a government watch list, which prevents him from entering the cockpit.[19] Sherfen is not the only innocent person placed on a terror watch list. Others individual who are either on a list or mistaken for those on the list include a former Assistant Attorney General, many individuals with the name Robert Johnson, the late Senator Edward Kennedy and even Nelson Mandela.[20]

The most recent case – revealed just last week – is that of Mikey Hicks, an 8 year old boy who has been on the selectee list seemingly since birth. According to Hicks' family their travel tribulations that began when Mikey was an infant. When he was 2 years old, the kid was patted down at airport security. He's now, by all accounts, an unassuming bespectacled Boy Scout who has been stopped every time he flies with his family.[21]

---

[18] John Solomon, *Bureaucracy Impedes Bomb Detection Work*, Washington Post, Aug. 12, 2006, at: http://www.washingtonpost.com/wp-dyn/content/article/2006/08/12/AR2006081200269.html

[19] Jeanne Meserve, *Name on government watch list threatens pilot's career*, CNN.com, August 22, 2008, http://www.cnn.com/2008/US/08/22/pilot.watch.list/index.html?iref=newssearch

[20] For details on these individuals and many other please see: http://www.aclu.org/technology-and-liberty/unlikely-suspects

[21] Lizette Alvarez, *Meet Mikey, 8: U.S. Has Him on Watch List*, New York Times, January 13, 2010.[22] *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program, Department of Homeland Security*,

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00250 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.057

In addition, to stops at the airport watch list information is also placed in the National Criminal Information Center database. That means law enforcement routinely run names against the watch lists for matters as mundane as traffic stops. It's clear that innocent individuals may be harassed even if they don't attempt to fly.

Nor is there any due process for removing individuals from the list – there is simply no process for challenging the government's contention that you are a terrorist. Even people who are mistaken for those on the list face challenges. A September 2009 report by the Inspector General of the Department of Homeland Security found that the process for clearing innocent travelers from the list is a complete mess.[22]

In light of the significant and ongoing harm to innocent Americans as well as the harm to our national security caused by the diversion of security resources these watch lists must be substantial reduced in size and fundamental due process protections imposed. Innocent travelers must be able to remove themselves from the list both for their sake and the sake of national security.

Aviation Screening on the Basis of Nationality

This history of the civil rights movement in the 20th and 21st Century is a long, compelling rejection of the idea that individuals should be treated differently on the basis of their race or nation of origin. Because of that, the administration's decision to subject the citizens of fourteen nations flying to the United States to intensified screening is deeply troubling. Longstanding constitutional principles require that no administrative searches, either by technique or technology, be applied in a discriminatory matter. The ACLU opposes the categorical use of profiles based on race, religion, ethnicity, or country of origin. This practice is nothing less than racial profiling. Such profiling is ineffective and counter to American values.

But the harm that profiling on the basis of national origin does to civil liberties is not an abstraction – it also has direct impact on American security interests. These harmful policies have a direct impact on the Muslim and Arab communities. The Senate Homeland Security and Government Affairs committee has heard testimony from several witnesses who cited the growth of Islamophobia and the polarization of the Muslim community as risk factors that could raise the potential for extremist violence.[23] Unfairly focusing suspicion on a vulnerable community tends to create the very alienation and danger that we need to avoid.

Office of the Inspector General OIG 09-10, September 2009. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf

[22] *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program, Department of Homeland Security*, Office of the Inspector General OIG 09-10, September 2009. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf

[23] *See for example*, Hearing of the Senate Homeland Security and Governmental Affairs Committee, *Violent Islamist Extremism: The European Experience*, (June 27, 2007), particularly the testimony of Lidewijde Ongering and Marc Sageman, available at: http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=9c8cf805-75c8-48c2-810d-d778af31cca6.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00251 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.058

Indeed a recent United Kingdom analysis based on hundreds of case studies of individuals involved in terrorism reportedly identified "facing marginalization and racism" as a key vulnerability that could tend to make an individual receptive to extremist ideology.[24] The conclusion supporting tolerance of diversity and protection of civil liberties was echoed in a National Counterterrorism Center (NCTC) paper published in August 2008. In exploring why there was less violent homegrown extremism in the U.S. than the U.K., the authors cited the diversity of American communities and the greater protection of civil rights as key factors.

At the January 7, 2009 White House briefing regarding the security failures surrounding the Christmas attack, DHS Secretary Janet Napolitano raised a question about "counter-radicalization."[25] She asked, "How do we communicate better American values and so forth, in this country but also around the globe?" Of course the Secretary should know American values are communicated through U.S. government policies, which is why adopting openly discriminatory policies can be so damaging and counterproductive to our national interests.

IV. Conclusion

Ultimately security is never absolute and never will be. It is not wise security policy to spend heavily to protect against one particular type of plot, when the number of terrorist ideas that can be hatched – not only against airlines, but also against other targets – is limitless. The President has identified a failure "connect the dots" by intelligence analysts as the main reason that Umar Farouk Abdulmutallab was able to board a flight to the U.S.[26] We must not lose sight of that reality. Limited security dollars should be invested where they will do the most good and have the best chance of thwarting attacks. That means investing them in developing competent intelligence and law enforcement agencies that will identify specific individuals who represent a danger to air travel and arrest them or deny them a visa.

Invasive screening mechanisms, enlarging already bloated watch lists, targeting on the basis of national origin – none of these approaches go to the heart of what went wrong on Christmas day. Instead they are a dangerous sideshow – one that harms our civil liberties and ultimately makes us less safe.

---

[24] Alan Travis, "*MI5 Report Challenges Views on Terrorism in Britain*," The Guardian, (August 20, 2008) *at*: http://www.guardian.co.uk/uk/2008/aug/20/uksecurity.terrorism1 *and;* Alan Travis, "*The Making of an Extremist*," The Guardian (Aug. 20, 2008) *at*: http://www.guardian.co.uk/uk/2008/aug/20/uksecurity.terrorism

[24] National Counterterrorism Center Conference Report, Towards a Domestic Counterradicalization Strategy, (August 2008)

[25] Briefing by Homeland Security Secretary Napolitano, Assistant to the President for Counterterrorism and Homeland Security Brennan, and Press Secretary Gibbs, 1/7/10, at: http://www.whitehouse.gov/the-press-office/briefing-homeland-security-secretary-napolitano-assistant-president-counterterroris

[26] Jake Tapper and Sunlen Miller, *Obama: Intelligence Community Failed to "Connect the Dots" in a "Potentially Disastrous Way"*, ABCNews.com, January 05, 2010. http://blogs.abcnews.com/politicalpunch/2010/01/obama-intelligence-community-failed-to-connect-the-dots-in-a-potentially-disastrous-way.html

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00252 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.059

Post-Hearing Questions for the Record
Submitted to the Honorable Michael E. Leiter
From Senator Daniel K. Akaka

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question 1: (U) According to the Intelligence Reform and Terrorism Prevention Act, strategic operational planning is "planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies." However, this may differ from what is being implemented since strategic operational planning is an unconventional term.

a. **How does the National Counterterrorism Center (NCTC) currently define strategic operational planning and has its definition evolved over time?**

b. **Do other U.S. Government departments and agencies involved in counterterrorism planning fully support you in the definition of strategic operational planning currently in use?**

c. **What priority does the Directorate of Strategic Operational Planning (DSOP) give to planning relative to other activities it may be involved in such as facilitation, negotiation, and mediation between the agencies involved in counterterrorism activities?**

Answer: **(U)** NCTC's Directorate of Strategic Operational Planning (DSOP) has taken its direction on the definition of strategic operational planning from both the Intelligence Reform and Terrorism Prevention Act (IRTPA), Executive Order (EO) 13354 (revoked by EO 13470 in July 2008), and from National Security Staff direction. DSOP views strategic operation planning as a process that develops interagency counterterrorism (CT) plans to help translate high level strategies and policy direction into coordinated department and agency activities. This process integrates all elements of national power by involving the appropriate department and agency representatives, to include those not traditionally associated with the CT mission.

(U) Since DSOP's creation, its definition of strategic operational planning has remained largely constant. However, the method for strategic operation planning has evolved to coincide with the lessons learned and the needs of the CT community. In its first three years, DSOP focused on broad, long-term strategic planning to provide common objectives, missions, and roles and responsibilities for CT departments and agencies. The National Implementation Plan for the War on Terror—approved by President George W. Bush in 2006 and 2008—was the first whole of government plan for CT and provided a common framework for department and agency CT actions. In addition to long-term strategic planning, DSOP has developed a capacity to conduct near-term interagency planning to respond to current threats.

(U) The lack of broad interagency understanding of DSOP's role and the term "strategic operational planning" has created some confusion and uncertainty among departments and

56838.060

agencies. However, recent DSOP-led planning efforts have been increasingly supported by departments and agencies—including those that are not traditionally CT-focused. NCTC is reviewing the Project on National Security Reform's conclusions on DSOP for potential ways of improving interagency participation.

(U) NCTC DSOP's focus remains on conducting strategic operational planning, using its mandate to develop whole of government CT plans to engage in cross-agency collaboration. The strategic operational planning process integrates all phases of the planning cycle—developing a plan, monitoring its implementation, and assessing its effectiveness—and creates communities of interest to coordinate and integrate implementation. Negotiation, facilitation and mediation are components of this interagency planning process.

56838.061

Hearing Date: 20 January 2010
Committee: SHSGAC
Member: Senator Akaka
Witness: Director Leiter
Question: 2

Question 2: (U) I asked you during the hearing about the relationship between the authorities of DSOP and the State Department's Coordinator for Counterterrorism (S/CT), which appear to overlap. Your response cited DSOP's statutory prohibition from directing operations.

a. How have DSOP and S/CT defined their relationship with one another given their similar legislative mandates?

b. Regarding operations, is it possible to plan counterterrorism activities proactively without being involved in directing them?

c. If so, how is DSOP accomplishing this?

Answer: (U) NCTC cooperates well with and recognizes the importance of a strong relationship with the State Department's Coordinator for Counterterrorism (S/CT). Although the authorities appear to overlap and the relationship is multifaceted DSOP regularly collaborates with S/CT to delineate responsibilities and avoid duplication. Specifically, DSOP directly supports the State Department's lead in developing regional CT strategic objectives, ensuring alignment with the National Implementation Plan and monitoring department and agency activities toward these objectives. When directed by the National Security Staff, DSOP develops near-term, threat-based CT plans, working closely with S/CT and the White House to ensure plans are consistent with broader foreign policy guidance. DSOP and S/CT have also forged a strong partnership on countering violent extremism.

(U) It is possible to conduct counterterrorism strategic operational planning without directing the execution of the resulting operation. NCTC has broad statutory authority to conduct strategic operational planning for counterterrorism activities and assigning roles and responsibilities to lead departments or agencies for counterterrorism activities in support of such strategic operational planning. NCTC is only precluded, by statute, from directing the execution of any operation resulting from such planning. DSOP creates collaborative interagency environments to increase transparency between, and provide strategic context for, departments' and agencies' operations. DSOP's collocation with the intelligence community allows integration of intelligence to support the development of clear strategic objectives and the alignment of USG current and planned activities to those objectives. NCTC DSOP does not direct the execution of operations, but by holding collaborative meetings and collecting data on both current and proposed actions from across the USG—to include the relevant operators in the field—NCTC DSOP facilitates a coordinated planning process for agencies with the appropriate authorities to execute operations.

56838.062

Hearing Date: 20 January 2010
Committee: SHSGAC
Member: Senator Akaka
Witness: Director Leiter
Question: 3

Question 3: (U) One of the President's preliminary conclusions regarding the failed attack is that failure to prevent the attempt was not the fault of a single individual or organization, but rather a failure across organizations and agencies. As you know, Congress gave the NCTC Director the responsibility to coordinate interagency counterterrorism planning. Do you believe that you have the full authority you need to direct U.S. Government agencies on this shared mission, or are further changes needed?

Answer: **(U)** Pursuant to Section 119 of the National Security Act of 1947, as amended, NCTC has as a primary mission the conduct of strategic operational planning for counterterrorism activities, integrating all instruments of national power. In connection with these strategic operational planning duties, NCTC is further charged with the mission of assigning roles and responsibilities to lead Departments or agencies for counterterrorism activities. NCTC, may not, however, direct the execution of counterterrorism operations.

(U) No formal conclusion has yet been drawn as to whether specific additional authorities are required to accomplish NCTC's interagency counterterrorism mission, but NCTC is continuing to evaluate—in conjunction with outside observers—three principal areas of possible remediation. First, NCTC is—pursuant to the President's tasking of January 7, 2010—developing a process to ensure follow up of threat information by the whole of the U.S. Government. In doing so, NCTC will seriously evaluate whether additional authorities, either through Executive Order or legislation, are necessary to fulfill the President's tasking. Second, NCTC will continue to evaluate whether existing information sharing policies and procedures are sufficient to provide adequate access to data relating to terrorism threats—in particular that data held by Departments and agencies outside the Intelligence Community (IC). Third, as roles and responsibilities for counterterrorism analysis are reaffirmed and clarified in response to the President's tasking of January 7, 2010, NCTC will continue to review whether it has the authorities necessary to ensure appropriate coverage of priority counterterrorism issues by the entirety of the IC.

(U) Finally, NCTC is reviewing the report from the Project on National Security Reform, "Toward Integrating Complex National Missions", and its recommendations for the Directorate of Strategic Operational Planning to inform consideration of necessary authorities for the conduct of strategic operational planning, including potential need for additional budgetary authority.

56838.063

Post-Hearing Questions for the Record
Submitted to the Honorable Michael E. Leiter
From Senator Susan M. Collins

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question 1: (U) The initial error in failing to accurately determine whether Abdul Mutallab had a valid visa was caused by a slight misspelling. This error is similar to the mistakes made by Customs and Border Protection in failing to identify a Mexican national with a multiple-drug-resistant form of Tuberculosis who was able to enter the U.S. twenty-one times, even after DHS had his last name and date of birth. With the Mexican national, DHS acknowledged that its border screening database was antiquated and lacked sophisticated search functions. After this Committee's hearing and investigation into that incident in 2007, I understand that these technological limitations were addressed. Director Leiter, your office has access to the Consolidated Consular Database that holds U.S. visa records. Do you know if this database has been enhanced to provide matches for searches with near, but not exact, name matches to accommodate for misspellings?

Answer: (U) NCTC is aware that State Department has taken measures to enhance Consolidated Consular Database name search capabilities. We have directed your query to the Department of State for a reply to be prepared and delivered directly to the Committee.

56838.064

Post-Hearing Questions for the Record
Submitted to the Honorable Michael E. Leiter
From Senator John Ensign

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2009

Question 1: (U) I understand that in order for someone to be moved from TIDE (Terrorist Identities Datamart Environment) to the TSDB Watchlist (Terrorist Screening Database) the government must have sufficient identifying information and must satisfy a "reasonable suspicion" standard. While the information provided by the terrorist's father alone did not satisfy the "reasonable suspicion" standard, the White House Review indicated that the NCTC along with the CIA did not search all available databases to uncover additional derogatory information that may have resulted in the terrorist being placed on the no-fly list.

- **Why didn't the NCTC search all the databases?**

Answer: (U) The response to this question has been delivered to the Office of Senate Security.

56838.065

Post-Hearing Questions for the Record
Submitted to the Honorable Dennis C. Blair
From Senator Daniel K. Akaka

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question 1: (U) In your response to my question about taking privacy and civil liberties into account when carrying out corrective actions in response to the December 25 terrorist attack, you stated that you believe the Privacy and Civil Liberties Oversight Board should be "manned up and started" and that it "would provide a very valuable service." Please elaborate on what benefits you believe this Board would have for the Intelligence Community and national security, and please state whether you have brought these benefits to the President's attention.

Answer: (U) The Privacy and Civil Liberties Oversight Board will provide advice and oversight with respect to efforts to protect the nation from terrorism. The Board is to consist of members from outside government (other than the chair, who is to serve on a full-time basis), with full access to relevant information. This perspective is important not only for helping to enhance our system of checks and balances, but also to engender increased trust among the American people in how the Intelligence Community operates.

(U) The Intelligence Community (IC) necessarily works in a classified environment. While this enables the community to mount successful intelligence operations, it also raises questions about our programs that we find difficult to answer in public settings. The IC remains subject to oversight and accountability nonetheless. We are subject to congressional oversight - a vital check and balance on intelligence activities. To the extent our activities are covered by the Foreign Intelligence Surveillance Act (FISA), for example, they require supervision by the FISA court. Moreover, we have internal oversight mechanisms, including those implemented through offices of general counsel, offices of inspector general, intelligence oversight offices, and privacy and civil liberties officers. For example, within my office, the Civil Liberties Protection Officer works closely with my staff including the General Counsel and the Inspector General, and those of other elements, to provide advice and oversight from a civil liberties and privacy perspective.

(U) We can also bring to bear external expertise to review our activities. That is what I did in naming former acting DCI John McLaughlin to lead a panel of national security experts, including my Civil Liberties Protection Officer, to review the Fort Hood and December 25 incidents, and provide me with recommendations consistent with protecting privacy and civil liberties.

(U) The Privacy and Civil Liberties Board would provide a welcome addition to this architecture for protecting privacy and civil liberties. With members drawn from outside government, it

56838.066

would bring an external perspective to counterterrorism activities. With the ability to access information, it would be able to gain an in-depth understanding of any program of its choosing. The Board would therefore be in a position to provide a degree of transparency that would enhance public confidence that the community is living up to its vision – to exemplify America's values - operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties.

Question 2: (U) One of the President's preliminary conclusions regarding the failed attack is that failure to prevent the attempt was not the fault of a single individual or organization, but rather a failure across organizations and agencies. As you know, Congress gave the Director of National Intelligence the responsibility to direct interagency intelligence efforts. Do you believe that you have the full authority you need to direct U.S. Government agencies on this shared mission, or are further changes needed?

Answer: (U) In the aftermath of the Fort Hood and Christmas Day attacks, and in response to the President's taskings, the Intelligence Community, under the leadership of the Director of National Intelligence, has undertaken several levels of review to determine how we can ensure that intelligence information is being accessed and shared properly, and what changes may be needed in order to better prevent such attacks. In the course of examining the results and recommendations from those reviews, we are assessing whether additional authorities are needed to carry out any proposed changes. If additional authorities are needed, we will incorporate requests for those authorities into a legislative proposal for consideration by Congress.

56838.067

Post-Hearing Questions for the Record
Submitted to the Honorable Dennis C. Blair
From Senator Susan M. Collins

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question 1: (U) The initial error in failing to accurately determine whether Abdul Mutallab had a valid visa was caused by a slight misspelling. This error is similar to the mistakes made by Customs and Border Protection in failing to identify a Mexican national with a multiple-drug-resistant form of Tuberculosis who was able to enter the U.S. twenty-one times, even after DHS had his last name and date of birth. With the Mexican national, DHS acknowledged that its border screening database was antiquated and lacked sophisticated search functions. After this Committee's hearing and investigation into that incident in 2007, I understand that these technological limitations were addressed. Director Blair, your office has access to the Consolidated Consular Database that holds U.S. visa records. Do you know if this database has been enhanced to provide matches for searches with near, but not exact, name matches to accommodate for misspellings?

Answer: (U) The State Department has taken measures to enhance Consolidated Consular Database name search capabilities. I have directed your query to them for a reply to be prepared and delivered directly to the Committee.

Question 2: (U) Director Blair, you have authority from the Intelligence Reform Act to direct analysts to focus on specific emerging threats. With the attack on the U.S. Embassy in Yemen in 2008 that killed 17 people, the attempted assassination of the chief counter-terrorism official in Saudi Arabia last August, and our government's expanded concern with al-Qaeda in the Arabian Peninsula, did you focus more analysts on this threat?

Answer: (U) The response to this question has been delivered to the Office of Senate Security.

56838.068

Post-Hearing Questions for the Record
Submitted to the Honorable Dennis C. Blair
From Senator John Ensign

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2009

Question 1: (U) The President's Review of the attempted Christmas Day attack indicated that "Information Technology within the counterterrorism community did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information." In his memo to Department Heads, the President specifically asked you to accelerate IT enhancements. What IT enhancements does your office have planned to address this shortfall? What enhancements have already been instituted?

Answer: (U) The response to this question has been delivered to the Office of Senate Security.

Question 2: (U) Top government officials revealed on February 2 that Abdulmutallab is cooperating with the FBI and may be providing useful information to authorities about al Qaeda. Is the United States Government plea bargaining for Intelligence? What type of precedent do you believe plea bargaining with terrorists' sets? How would we know if the intelligence gathered is credible?

Answer: (U) I respectfully refer you to the Department of Justice, which has indicted Mr. Abdulmutallab for federal crimes relating to his actions on December 25, 2009.

(U) Additional information responding to this question has been delivered to the Office of Senate Security.

56838.069

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Carl Levin

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question#:	1
Topic:	role
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), the National Counterterrorism Center (NCTC) serves as the primary organization in the U.S. Government for integrating and analyzing all intelligence pertaining to counterterrorism (except for information pertaining exclusively to domestic terrorism [which is the responsibility of the Federal Bureau of Investigation]). However, the Homeland Security Act of 2002, assigns the intelligence component of DHS with the responsibility to receive, analyze, and integrate law enforcement and intelligence information in order to "(A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities to the homeland."

What role does DHS have under law and in practice for evaluating threat streams and warning of possible terrorist attacks?

Response: The Homeland Security Act of 2002 assigns DHS the primary mission to "prevent terrorist attacks within the United States" and "reduce the vulnerability of the United States to terrorism." Pursuant to section 201(d) of the Act, DHS satisfies these requirements by analyzing all-source intelligence and information from DHS Component organizations, other Federal, state and local government agencies—including intelligence and law enforcement partners—and the private sector. This analysis is used to identify potential threats and to provide warnings of possible terrorist attacks, and indicators of terrorist tactics, techniques, and procedures.

DHS has the specific responsibility in 201(d)(9) "to disseminate" information it analyzes "... in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States." Pursuant to sec. 203 of the Act, DHS also "administer(s) the Homeland Security Advisory System...to provide advisories or

56838.070

Question#:	1
Topic:	role
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

warnings regarding the threat or risk that acts of terrorism will be committed on the homeland." In fulfilling these responsibilities, DHS consults with the DNI, the Intelligence Community, law enforcement, and other elements of the Federal government to establish collection priorities and strategies for information relating to terrorist threats [201(d)(9)], and with state and local governments and private sector entities to ensure information relating to terrorist threats is appropriately exchanged [201(d)(9)].

To this end, DHS produces a variety of analytical products for distribution to various customer sets, including intelligence assessments, Roll Call Releases, joint bulletins on time-sensitive events, reference aids, daily summaries, and tailored responses to inquiries. The Department also provides weekly, tailored briefings to its state and local customers, and ad hoc briefings to all its customers, as warranted.

Question: Specifically, regarding the intelligence that the President's summary states was available prior to the attempted bombing of NW-253, did DHS have access to that intelligence? That is, was the intelligence disseminated to DHS or was it available in databases to which DHS personnel had access? If so, what did DHS do with that information, or with the database access?

Response: Intelligence information relating to Umar Farouk Abdulmutallab was available to DHS and the entire Intelligence Community prior to December 25, 2009. Mr. Abdulmutallab was entered into the Terrorist Identities Datamart Environment (TIDE), maintained by the National Counterterrorism Center. However, the derogatory information associated with that record, based on the policy in place at that time, was insufficient for him to be watchlisted through the Terrorist Screening Database (TSDB, the U.S. Government's consolidated terrorist watchlist). It was also insufficient to have him placed on the No Fly list which would have prevented him from boarding, or subjected him to additional screening prior to boarding Northwest Flight 253. At the time of his travel, a Consolidated Lookout and Support System (CLASS) notice had been posted for Mr. Abdulmutallab, but these records did not meet the criteria for referral to IAP officers in Amsterdam prior to boarding. Since this incident, CBP has added CLASS lookouts with terrorism-related indicators to the pre-departure vetting criteria.

While in flight, U.S. Customs and Border Protection (CBP) officers in Detroit conducted a screening of inbound flights against a consolidated system that included the State Department's CLASS database. Mr. Abdulmutallab was identified as a match to the record and CBP officers were awaiting his arrival to conduct an in-depth interview.

56838.071

Question#:	2
Topic:	NCTC
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: What presence does DHS have at NCTC and what functions do DHS analysts perform there?

How do DHS analysts at NCTC interact with their counterparts at the DHS Office of Intelligence and Analysis and with the intelligence staffs of the DHS components? Are DHS personnel at NCTC permitted to share what they learn, or have access to, at NCTC with DHS officials in DHS's operational components? If not, why not? Should this be corrected?

Response: DHS currently has 17 analysts assigned to the National Counterterrorism Center (NCTC), as broken out below:

- Office of Intelligence and Analysis (I&A) – 11
- National Protection and Programs Directorate – 1
- United States Citizenship and Immigration Services – 1
- United States Coast Guard - 4

In general, analysts detailed to NCTC operate as NCTC employees, not as DHS liaisons, and they are fully integrated into NCTC's analytic management structure. While these analysts maintain reach-back capabilities and apply their expertise and experiences in Homeland intelligence analysis to the intelligence topics they are assigned, their roles are determined by NCTC management. The analysts have individual analytic accounts for which they are responsible, and have full access to intelligence available to other analysts in NCTC.

DHS analysts assigned to NCTC share intelligence and coordinate with DHS under NCTC's guidelines, as appropriate with the parameters of the clearance levels and need-to-know of counterpart DHS analysts. Coordination is generally accomplished through I&A, with I&A performing any onward coordination with the Intelligence Enterprise within those same parameters.

Among I&A's contribution to NCTC are two detailees to the Interagency Threat Assessment and Coordination Group (ITACG), as well as three individuals from state, local, and tribal organizations, who are "federalized" as I&A employees and detailed to NCTC. Rather than being integrated into an NCTC work unit, one I&A detailee leads the ITACG under NCTC's management, and the second serves as a senior analyst supporting the ITACG mission. The federalized detailees from state, local, and tribal organizations

56838.072

Question#:	2
Topic:	NCTC
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

serve as the ITACG's core, providing crucial advice and insights into state, local, and tribal needs and interests. Each of these detailees has access to NCTC systems, but his work focuses on reviewing finished production, rather than original intelligence analysis. Each works with all agencies that support intelligence collection and dissemination from within the NCTC analytical offices to ensure that relevant information is shared with state and local customers.

Under NCTC's information sharing guidelines, because NCTC has direct access to many sensitive compartmented systems from across the federal government, NCTC employees – including DHS detailees – are necessarily constrained from sharing information derived from those sources, pursuant to arrangements with the agencies that own them. NCTC's guidelines in this regard raise issues for DHS under the following circumstances:

- When DHS analysts co-author or provide significant input to an NCTC product based on unique Homeland equities, lack of access to all relevant materials can skew otherwise valuable and relevant input we can provide.
- When DHS analysts are assigned to specialized projects at NCTC, as opposed to a routine detail to an NCTC analytic team, we believe that these guidelines should be reconsidered so that the analyst has the authority to maximize reachback to contribute Homeland inputs.

A direct line of communication and information exchange in a 24/7 basis must be created between the NCTC and the DHS National Operations Center (NOC). NOC employees must be fully integrated within the Intelligence Community (IC) and able to contact and exchange intelligence information with the NCTC independently from DHS I&A.

In addition to this a Congressional study must analyze which counterterrorism functions currently under the FBI National Security Branch must be better placed under DHS I&A and DHS NOC. Those functions must be transitioned to DHS within a period 6 months from the date of the study.

56838.073

Question#:	3
Topic:	ATS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: CBP uses the Automated Targeting System (ATS) at its National Targeting Center to identify high risk passengers and cargo shipments. The passenger component of ATS processes traveler information against other information available to ATS and applies threat-based scenarios comprised of risk-based rules to assist CBP officers in identifying individuals who require additional screening or in determining whether individuals should be allowed entry into the United States. It was reported that CBP officers learned of Abdulmutallab's possible extremist links while NW-253 was airborne on December 25 as a result of cross-checking his name with the State Department's CLASS database. As a result, CBP officers intended to question him when he landed.

Was the determination to question Abdulmutallab upon landing based on the risk-based rules within the ATS system or purely on the CLASS entry or other intelligence information?

Response: Based on the Department of State (DOS) record, Abdulmutallab would have been referred to secondary inspection upon his arrival in Detroit. The risk-based rules in the ATS passenger module are designed to identify higher-risk travelers whose travel parameters match threat-based scenarios, but who do not have pre-existing lookout records.

Question: Why was the CBP security assessment of passengers for NW-253 not completed prior to departure of the flight?

Response: CBP assessments are an on-going process that generally start 72 hours prior to a flight's departure when Passenger Name Record (PNR) information from the airlines reservation system is transmitted to CBP and processed in the Automated Targeting System – Passenger (ATS-P) to the passenger's arrival at a U.S. airport. Beginning at 72 hours CBP can identify potential watchlist matches and patterns of illicit activity through the analysis of PNR. PNR data can be carrier reservation data and so is not standardized. As a result, a given PNR record may not always have full information on a traveler. For example, travel document information or method of payment may not be present. Once Advance Passenger Information (API) is received from the airline, prior to the flight's departure (API contains complete biographic information taken from the passenger's travel document at check-in) the passenger manifest is processed through the risk-based rule scenarios in ATS-P and additional lookouts may be found or possible lookouts may be confirmed. In the NW 253 case there were no records available to ATS-P that would have warranted CBP intervention to prevent Abdulmutallab from boarding the flight

56838.074

Question#:	3
Topic:	ATS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

because the State Department record present did not rise to the level of pre-departure vetting. In particular, the failure of the USG to watchlist Abdullmutallib hampered CBP's ability to take action prior to departure.

Question: Is it standard practice to cross-check passenger lists as soon as they are received (e.g., up to 72 hours in advance of departure) against the entire TSDB and the NCTC TIDE database? Was that done in this case? Should this be standard procedure?

Response: CBP utilizes the Advance Passenger Information System to screen passenger manifest data against the TSDB, including the No Fly and Selectee lists, but not TIDE. CBP automated checks also include (the U.S. Government's consolidated terrorist watchlist), as well as visa revocation records, Electronic System for Travel Authorization (ESTA) denials, lost/stolen passport records, public health records, and other information. As a result of gaps identified from the NW 253 incident, Department of State records related to terrorism are now also included in the initial security screenings prioritized for action by the ATS-P Hot List. The TIDE database is a classified repository that contains the underlying derogatory information on persons who are watchlisted in the TSDB. Subjects in the TIDE are included in the TSDB when they meet the interagency defined and agreed to criteria for terrorist watchlisting.

Question: If the CBP security assessment of passengers had been completed prior to departure, would Abdulmutallab still have been allowed to board?

Response: If CBP had conducted a pre-departure screening which included vetting against the Department of State's records related to terrorism it is possible that Abdulmutallab would still have been permitted to board the aircraft, because there were no significant lookouts in the systems, e.g. no visa revocation by Department of State and neither TSDB nor No Fly/Selectee record.

Question: Would he have been subjected to additional screening or questioning?

Response: At the time the Advance Passenger Information data was provided to CBP, the record in TECS for Abdulmutallab that had been received from State was not coded as a TSDB or terrorist related record, and CBP's Automated Targeting System did not flag him as requiring additional screening by CBP IAP officers at Amsterdam-Schiphol International Airport. Since December 25, CBP has modified its automated screening procedures to identify State Department records pertaining to terrorism which results in additional screening.

Question: Were there DHS personnel at the departing airport?

56838.075

Question#:	3
Topic:	ATS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Response: Yes, Abdulmutallab would have received additional screening prior to departure from Amsterdam and upon arrival at the port of entry.

Question: Had the security assessment been completed on the basis of the passenger list provided 72 hours in advance, could DHS personnel have traveled to Amsterdam to interview Abdulmutallab if they were not already there?

Response: IAP officers were on-site at Amsterdam. At the time the Passenger Name Record data was provided to CBP, the record in TECS for Abdulmutallab that had been received from State was not coded as a TSDB or terrorist related record, and CBP's Automated Targeting System did not flag him as requiring additional screening by CBP IAP officers at Amsterdam-Schiphol International Airport.

Since this time, CBP has changed its procedures so that it now focuses on identifying high-risk passengers and other inadmissible aliens prior to travel in an effort to prevent their departure prior to boarding commercial carriers bound for the United States from non-IAP overseas locations. CBP does this for IAP and non-IAP locations, by identifying all passengers who are possible matches to Terrorist Screening Database (TSDB including No Fly List records), Electronic System for Travel Authorization (ESTA) denials, Visa Revocation, Public Health, Lost or Stolen Passports (non-US) hits and all Department of State TECS records with terrorism related exclusion.

The CBP National Targeting Center-Passenger (NTC-P) coordinates with IAP offices, Immigration Customs Enforcement (ICE) Attachés, CBP Attachés, and the Regional Carrier Liaison Group (RCLG) to assist with notifying specific airlines and that these identified subjects do not board an aircraft destined to the United States.

56838.076

Question#:	4
Topic:	CAPPS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Were the passengers on NW-253 screened through the Transportation Security Administration's Computerized Passenger Pre-Screening System (CAPPS) or other DHS computer-assisted risk analysis capabilities? If not why not?

Response: The passengers aboard NW 253 were screened against CBP's Automated Targeting System-Passenger.

56838.077

Question#:	5
Topic:	criteria
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Carl Levin
Committee:	HOMELAND SECURITY (SENATE)

Question: Does the Computer-Assisted Passenger Prescreening System (CAPPS) or other Department of Homeland Security (DHS) computer-based analysis system's screening algorithms include any current intelligence information, or is it based solely on criteria such as a passenger's nationality, ticketing, itinerary, frequent flyer status, etc.? Do the DHS organizations that operate these risk-analysis tools have access to intelligence databases, or are there intelligence agency personnel detailed there who can search the intelligence holdings of their home agencies? If not, why not? Why not conduct risk analysis against all the data at the government's disposal?

Response: The Department of Homeland Security (DHS) has computer-based algorithms in place that are informed by intelligence and operational information. These algorithms utilize available passenger data. The DHS organizations that operate these algorithms – which include Intelligence and Analysis (I&A), the Transportation Security Administration, and the U.S. Coast Guard – have direct access to intelligence databases as well as Intelligence Community (IC) agencies. DHS also has personnel detailed to IC agencies under various agreements and understandings. DHS conducts terrorism risk analysis by leveraging the most relevant data available, including all source intelligence information.

56838.078

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Daniel K. Akaka

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question#:	6
Topic:	VSP - 1
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, Immigration and Customs Enforcement's (ICE's) Visa Security Program deploys special agents to high-risk visa activity posts to conduct in-depth reviews of individual visa applicants. In 2005, the Government Accountability Office observed that these agents would benefit from greater language proficiency for interviewing applicants and reviewing files. Likewise, a 2008 Department of Homeland Security (DHS) Inspector General report stated that language skills appear to be very important at some posts.

Since these reports were issued, has DHS made any changes to the language training and proficiency requirements for ICE's Visa Security Officers? If so, please describe these changes. If not, please discuss whether DHS plans to review the requirements and any anticipated changes to them.

Response: DHS has participated in language training as recommended by the DHS IG report. For example, Special Agents assigned to Jakarta, Indonesia attended language training at the Department of State's Foreign Service Institute prior to deploying to post. In some instances, DHS has been able to assign agents proficient in a language to a particular post. This was the case in both Manila and Frankfurt. ICE has recently made language training available through a contract with Rosetta Stone. This training is available to Special Agents both before and during their overseas deployments. Additionally, all ICE offices with Visa Security responsibilities hire locally engaged staff who are proficient in the local language and who are available to assist in interviewing applicants and reviewing files.

56838.079

Question#:	7
Topic:	resources
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The Transportation Security Administration's (TSA) Office of Global Strategies develops and promotes effective transportation security processes worldwide. It relies on its overseas TSA representatives to align security between the U.S. and foreign governments and to assess foreign airports and air carriers. Since the Christmas Day attempt, what is DHS doing to ensure TSA has adequate staff and resources to reduce aviation security risks before they reach our shores?

Response: The President's budget proposal for fiscal year (FY) 2011 reflects an increase of $38.8 million for TSA's Office of Global Strategies (OGS) to support international outreach efforts, conduct assessments of international airports and inspections of foreign and domestic air carriers with flights to and from the United States, provide necessary security training to foreign governments, and evaluate the data identified through the assessment process in order to develop more robust systems and processes to better analyze the risk and institute appropriate security measures to prevent and deter terrorist acts. The requested resources will enable TSA to increase staffing levels by an additional 34 Transportation Security Specialists, 10 International Industry Representatives, 20 desk officers/analysts to support field operations, trend and risk analysis, and provide overall program support, and 10 personnel for Aviation Security Sustainable International Standards Teams and Rapid Response Teams. TSA will fund an additional three (3) Transportation Security Administration Representatives from existing resources.

56838.080

Question#:	8
Topic:	scanning
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: There were recent media reports that whole body imaging and related scanning technology may not detect small amounts of explosives. Please discuss the extent to which these concerns are valid. If needed, please provide any classified information to my staff through Senate Security.

Response: Advanced Imaging Technology (AIT) systems provide TSA with added capability to address explosives (bulk, liquids, and powders), as well as both metallic and nonmetallic weapons and prohibited items, based on the Transportation Security Officer's (TSO) visual interpretations of passenger imagery. The detection capabilities of TSA's AIT and related scanning technologies is sensitive information and can be provided to the Committee in the appropriate forum.

56838.081

Question#:	9
Topic:	WBI
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: In President Obama's January 7, 2010, memo about the attempted attack on Christmas Day, he assigned you with the task of "aggressively pursuing enhanced screening technology consistent with privacy and civil liberties." As you know, some privacy groups have argued that current whole body imaging technology may be too invasive.

Are DHS and TSA looking into whole body imaging equipment that may be less invasive but just as effective, such as passive millimeter wave technology?

Some small businesses may not have the capital to produce additional units of promising whole body imaging technology to support DHS and TSA testing and evaluation requirements. How are DHS and TSA handling this issue, and are they providing any funding to support the testing and evaluation of promising technology developed by small businesses?

Response: The Transportation Security Administration (TSA) continues to evaluate different Advanced Imaging Technologies (AIT), including passive millimeter wave units, as part of the ongoing acquisition process for these systems. During this process TSA continues to seek effective technologies that protect travelers' privacy and civil rights and civil liberties. Currently, Transportation Security Officers (TSOs) view AIT images from a remote location and have no contact with the passenger. Further, the AIT images are partially obscured by installed privacy algorithms and images are not stored. TSA is working with the Department of Homeland Security's Science and Technology Directorate (DHS S&T), the security industry, and international government partners to develop an automated threat detection capability. The objective of Automated Target Recognition detection algorithms is to provide effective detection performance without the need for TSOs to interpret the passenger imagery to identify potential threat items. Instead, the technology would flag anomalies for further TSO screening on a representative image of the human body.

In order to adequately evaluate the system performance of any technology, TSA requires a certain quantity of systems from vendors for test and evaluation. This is especially important during the operational testing of technologies, where technologies must be tested at a variety of airports with different operators, travel characteristics (type of baggage, passenger clothing, etc.) and physical environments (altitude, humidity, temperature, etc.). While TSA tries to limit the number of systems requested from vendors for testing, the aggressive acquisition, budgeting, and deployment schedules that are required to ensure a timely rollout of security technologies often require simultaneous testing at multiple laboratories and airports. Additionally, as pertains to funding for testing, the DHS S&T conducts all research and development for the TSA, including providing funding for the development and testing of emerging technologies.

56838.082

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Susan M. Collins

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question#:	10
Topic:	database
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: The initial error in failing to accurately determine whether Abdulmutallab had a valid visa was caused by a slight misspelling. This error is similar to the mistakes made by Customs and Border Protection in failing to identify a Mexican national with a multiple-drug-resistant form of Tuberculosis who was able to enter the U.S. twenty-one times, even after DHS had his last name and date of birth.

With the Mexican national, DHS acknowledged that its border screening database was antiquated and lacked sophisticated search functions. After this Committee's hearing and investigation into that incident in 2007, I understand that these technological limitations were addressed.

Secretary Napolitano, the Department of Homeland Security has access to the Consolidated Consular Database that holds U.S. visa records. Do you know if this database has been enhanced to provide matches for searches with near, but not exact, name matches to accommodate for misspellings?

Response: TECS and Automated Targeting System algorithms are established to provide appropriate levels of matching for advance passenger information, primary, and secondary passenger screening.

CBP continuously evaluates and enhances matching algorithms to ensure levels of flexibility and sensitivity to provide users with appropriate matches. In particular, CBP's TECS Modernization effort is looking at options for new and enhanced matching algorithms.

56838.083

Question#:	11
Topic:	VSP - 2
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: At the hearing, I questioned you about delays in obtaining final DHS approval for the expansion of ICE's Visa Security Program to three State Department consular posts overseas. In response to my questions, you stated that you were unsure how long the requests for deployment to these posts had been waiting for your approval. When did the Secretary's Office receive each of the requests? And when did you approve them?

Response: The below chart indicates the dates on which ICE submitted five NSDD-38 applications to DHS for approval, and the corresponding dates on which DHS approved the respective applications.

ICE Attaché Office - VSP	NSDD-38 Sent to DHS for Approval	DHS Approval Date
Sana'a, Yemen	**9/8/2008**	**1/14/10**
Frankfurt, Germany	**9/25/2009**	**1/14/10**
Amman, Jordan	**9/25/2009**	**1/14/10**
Tel Aviv, Israel	**9/25/2009**	**1/15/10**
Jerusalem	**9/25/2009**	**1/15/10**

56838.094

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Tom Coburn

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question#:	12
Topic:	GAO
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In October, The Government Accountability Office (GAO) released a report on the Transportation Security Administration's (TSA) airport passenger screening technology. In the report, GAO recommends that the TSA "ensure that technologies have completed operational tests and evaluations before they are deployed."

What is the process for testing airport screening technology before it is deployed?

Do all airport screening technologies go through this process?

Please describe how long and what type of operation scenarios do you recreate to test this machines.

Response: The Transportation Security Administration (TSA) implements a robust Testing and Evaluation (T&E) program in accordance with Department of Homeland Security (DHS) policy and management directives to ensure that the operational effectiveness and suitability of candidate security technology systems are evaluated in both a laboratory and field environment prior to deployment. This process leverages data from multiple developmental and operational testing sources, accredited vendor data, modeling and simulation, and other special analyses (as required), in accordance with T&E and systems engineering principles and best practices. Security technologies undergo laboratory testing to verify conformance with technical standards and requirements, which includes requirements for probability of detection, false alarms rates, screening/decision time, health and safety, privacy, human factors engineering, etc. Laboratory testing is conducted primarily at the DHS Science and Technology Directorate's Transportation Security Laboratory in Atlantic City, NJ, but may also take place at a variety of other facilities, such as the Department of Defense laboratories or the Department of Energy National Laboratories. Depending on the technology, the TSA may also utilize the TSA Systems Integration Facility (TSIF, located in Arlington, VA) to conduct additional operational scenario and Concept of Operations testing on security

56838.085

Question#:	12
Topic:	GAO
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

technologies before they are fielded. Operational testing and evaluation (OT&E) is typically conducted within the intended field environment (typically, multiple aviation facility checkpoints) for a period of 30-60 days, with representative Transportation Security Officers (TSOs) operating under the intended concept of operations. OT&E testbed sites are chosen based on their ability to reflect the anticipated utilization rates, operational tempos, and mix of passengers and carry-on items representative of the intended deployment. In addition, threat surrogates are employed to the extent practical as part of the OT&E effort, to gauge system performance in a more realistic environment. Testing results are then compiled and analyzed. A determination is then made as to the overall operational effectiveness and suitability. These results are briefed to TSA leadership, the DHS Director of Operational Test and Evaluation (for oversight programs), and the relevant Acquisition Review Board.

56838.086

Question#:	13
Topic:	puffer
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Which versions of the explosive trace portal devices, also known as "puffer machines" have operational testing and which ones did not? Were they operationally tested and for how long? Did TSA have problems with the machines during operational testing? If they were not tested was there an official reason for that?

Response: Both fielded versions/vendors of the Explosives Trace Portal (ETP) were tested in an operational setting prior to full scale deployment. The Transportation Security Administration (TSA) proceeded with airport operational assessments by fielding five (5) commercial General Electric (GE) Entry Scan ETP systems in 2004. TSA proceeded with another round of operational assessments at multiple airports from April to May 2005 on both the GE and Smiths Sentinel II ETP to further validate operational suitability. Field test results demonstrated satisfactory performance, indicating the equipment was ready for full scale deployment. In April 2006 TSA began deploying ETPs to airports.

In 2006, TSA initiated another round of laboratory testing of the ETP to evaluate its effectiveness in detecting live explosives. During April and May of 2006, Idaho National Engineering and Environmental Laboratory conducted testing on both vendor submissions, which revealed a significant deficiency in the GE ETP's ability to detect certain explosive compounds. Once these test results were received, along with exhibited reliability, maintainability, and availability issues with the fielded units, TSA formally notified the ETP vendor in June of 2006 that TSA would not deploy any additional ETPs until the detection capabilities and reliability issues were addressed. Remaining delivery units were diverted to the TSA warehouse until improvements could be completed and verified.

56838.087

Question#:	14
Topic:	plans
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: I am concerned that our screening efforts may be chasing the last threat rather than the next one. In the Wall Street Journal, put it succinctly when he said, "to inspect all shoes after the shoe bomber almost succeeded, or to pat down passengers after the underwear bomber almost succeeded, provides no defense against the next techniques that could be tried at any time." Has TSA developed a comprehensive airport passenger screening plan that not only looks at present day threats but also looks down the road at newer threats?

Response: The Transportation Security Administration (TSA) considers this question to be central to its mission. Terrorist adversaries are highly adaptive and have shown they are capable of exploiting vulnerabilities in the aviation system. TSA employs a layered risked based security strategy to counter specific and general threats.

The use of intelligence informs TSA on the development of countermeasures to mitigate future threats. Over the past year, TSA has developed two inter-related processes increasing the likelihood that deployed countermeasures will mitigate both current and emerging threats. TSA has developed a risk analysis capability to assist resource allocation. In addition, TSA has developed a risk-based "capability-gap" process to identify the gaps between current capabilities and those needed to mitigate a portfolio of threat scenarios, including emerging threats. Through both risk analysis and the capability-gap process, TSA deploys "threat-agnostic" countermeasures capable of addressing a broader set of threats because their security design does not rely on assumptions about what form the threat might take. For example, Behavior Detection Officers (BDO) look for anomalous behaviors rather than a particular explosive or weapon. As a result, BDOs have a broader range of threat coverage and are less dependent on an assumption of which weapon terrorists will use in order to provide effective security.

In addition, TSA works with the Department of Homeland Security's Science and Technology Directorate and industry to advance the detection capabilities and operational suitability of a wide variety of screening technologies. TSA continues to support the development of emerging technologies that offer advanced screening capabilities while minimizing impact to the traveling public.

56838.088

Question#:	15
Topic:	testing
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: TSA is currently deploying whole body imagers in airports. Have the whole body imagers that TSA plans to purchase in 2010 been operationally tested and for how long?

Response: The Transportation Security Administration (TSA) has been testing and evaluating Advanced Imaging Technology (AIT) for almost three years. Through covert testing, ongoing airports assessments, developmental testing in a laboratory environment, and operational testing in the field environment, AIT has proven itself as an effective tool to assist TSOs with the detection of metallic and nonmetallic threats in the laboratory and in the field. Initial product demonstrations and laboratory testing were conducted at the Transportation Security Laboratory from February to May 2007. Operational testing of AIT included:

- Initial product demonstrations and laboratory testing at the Transportation Security Laboratory from February to May 2007;
- Operational utility evaluations (OUEs) at multiple airports from August 2007 to July 2008
    a. Sept 2007 – TSA awarded contracts for a limited number of systems to millimeter wave (MMW) and backscatter manufacturers for preliminary deployments to support extended surveillance
    b. MMW OUEs and field trials from November to December 2007 at Phoenix Sky Harbor International Airport (PHX); May to June 2007 at Los Angeles International Airport (LAX) and John F. Kennedy International Airport (JFK)
    c. Backscatter field trials OUEs from February to April 2008 at PHX; June 2008 at LAX; and July 2008 at JFK.
- Summer 2009 – Conducted Operational Testing and Evaluation (OT&E) and field trials of next-generation (AIT-2) MMW at George Bush Intercontinental Airport (IAH), Cleveland Hopkins International Airport (CLE), and Burbank-Glendale-Pasadena Airport (BUR); AIT-2 backscatter systems at IAH, CLE, and Greater Rochester International Airport (ROC) which provided the basis for recent procurement decisions.

TSA continues to evaluate other vendors' AIT proposals.

56838.089

Question#:	16
Topic:	devices
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Are all the airport screening devices purchased under the American Recovery and Reinvestment Act being operationally tested?

Response: Yes, all airport screening devices purchased under the American Recovery and Reinvestment Act undergo laboratory (developmental) testing as well as operational testing and evaluation in the field. They also meet the Transportation Security Administration's established requirements for each specific technology.

56838.090

Question#:	17
Topic:	health
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: As a doctor, I am concerned with the possible health effects associated with whole body imagers. Have the whole body imagers that TSA plans to purchase been tested for possible exposure to unhealthy levels of radiation or other health hazards?

Response: In its solicitation, the Transportation Security Administration references nationally recognized applicable safety standards for various forms of Advanced Imaging Technology (AIT). Vendors are required to demonstrate compliance to these standards prior to entering laboratory trials. Backscatter imaging results in exposures of less than 10 microREM. This is equivalent to the exposure each person receives in about 2 minutes of airplane flight at altitude or every 15 minutes from naturally occurring background radiation. The technology meets the American National Standards Institute standard for personnel security screening systems using X-rays. Millimeter wave AIT systems are also safe, utilizing energy frequency levels that are 10,000 times less than what is permitted for a cell phone. The average exposure time for a passenger being scanned by a millimeter wave AIT system is far less than the time that the average citizen is exposed to higher frequency cell phone transmissions throughout the day.

56838.091

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator John Ensign

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

Question#:	18
Topic:	decision
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that domestic flights in the air on Christmas night were not made aware of the emergency security directive. What was the reasoning for only alerting inbound transatlantic flights of the new directive? Who ultimately makes that decision?

Response: After being made aware of the incident onboard Northwest Flight 253, the Transportation Security Administration (TSA) convened a Senior Leadership Team Conference Bridge to evaluate the incident and order appropriate action. Based upon our understanding of the incident and related intelligence at the time and advice from the Federal Aviation Administration on the number of flights in-bound, the Acting Assistant Secretary ordered that flights to the United States from European locations be apprised of the incident. As we continue to evaluate our response to the NW 253 incident, we are reviewing our protocols to notify aircraft in the air.

In addition, TSA ordered additional security measures on these flights as well. As our response to the incident progressed, TSA expanded additional security measures to all international flights to the United States. Within five hours of issuing a Security Directive and Emergency Amendment ordering these measures, approximately 95 percent of our partners reported being in full compliance.

56838.092

Question#:	19
Topic:	directive
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: On January 4, TSA issued a new security directive to focus on more extensive screening of passengers flying from certain countries of interest. Was this decision made based on intel gathered from the Christmas Day terrorist himself or from other outside intelligence?

Response: The countries of interest listed in the Transportation Security Administration's Security Directive issued subsequent to the December 25, 2009, incident were selected based on information contained in Chapters Three (State Sponsors of Terrorism) and Five (Terrorist Safe Havens) of the State Department 2008 Country Reports on Terrorism, as well as information provided in Department of Defense country threat assessments. Additionally, two countries were identified based on a number of threat and aviation security factors. The list was coordinated with the U.S. State Department.

56838.093

Question#:	20
Topic:	briefing
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I understand that White House counterterrorism advisor John Brennan was briefed in October on an assassination attempt by Al Qaeda that may have used the same underwear bombing technique used on Christmas Day.

Question: Were you made aware of this briefing?

Response: Yes.

Question: What actions did DHS take in light of this new potential threat?

Response: DHS acts quickly in response to the identification of new and emerging threats, coordinating with the Intelligence Community, and across the DHS components, on products designed to inform and educate our state, local, and private sector partners. DHS continues to analyze this and other terrorist tactics, techniques, and procedures, and shares information via briefings, teleconferences, and the generation of products at the classified and unclassified levels.

In response to the attempted assassination briefed to John Brennan in October, DHS drafted a classified assessment for situational awareness, and an unclassified note that described the incident and subsequent extremist chatter encouraging the use of the device which the extremists lauded as an internally packed device. In response to the extremist chatter and initial press reporting, the Department undertook studies to determine the attenuation effects of the human body on an explosive detonation, and to determine the potential for TSA deployed technologies to detect such a device.

DHS has established research and development programs to address emerging threats and continues to invest in the development of advanced screening technologies. DHS has also recently established the DHS – Department of Energy (DOE) Aviation Security Enhancement Partnership to advance technical solutions to key aviation security problems in support of priorities announced by the President following the failed Christmas Day bombing attempt. While DHS has always worked in close collaboration with the DOE National Laboratories, the Department has now agreed to create a senior-level (at the Under Secretary level) governance mechanism to manage ways to extend and leverage this relationship with a focus on improving aviation security.

56838.094

Question#:	21
Topic:	IG
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: Last year, the DHS Inspector General issued a report and indicated that TSA's limited use of the No Fly and Selectee lists is appropriate in identifying individuals who pose threats to aviation security. Do you agree with the IG's assessment?

Response: The Transportation Security Administration (TSA) provided input to the Department of Homeland Security Office of Inspector General's assessment and TSA agreed that the use of the No-Fly and Selectee lists was appropriate in identifying individuals who posed threats to aviation security under normal circumstances.

DHS is collaborating with our interagency partners to assess corrective actions to protocols and procedures for watchlisting, as directed by the President, to ensure that gaps identified from this incident are addressed.

56838.095

Question#:	22
Topic:	DOS
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: In November, the State Department provided intel to the National Counterterrorism Center (NCTC) about information provided by the terrorist's father who expressed concerns with son's possible "extremist views". This information, however, did not state that Abdulmuttalab had a U.S. visa.

Do you feel that the State Department should have provided this information?

Response: We are confident all members of the Intelligence Community will build upon the lessons learned from the failed Abdulmutallab attack. Recent events highlight the need to regularly assess all aspects of the intelligence—planning, collection, processing, analysis, and dissemination—to fix process and procedures that fail and to bolster process and procedures that work.

Question: Do you believe that the State Department is the right entity to be issuing visas given the security issues?

Response: DHS notes the Department of State has served as the visa issuing authority for the U.S. Government with distinction. They have the infrastructure, resources, processes, and procedures to continue to do so.

56838.096

Question#:	23
Topic:	VSP - 3
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: The DHS Visa Security Program sends agents to posts overseas to review visa applications. I understand that in order to have the units deployed overseas, you must receive approval from the Department of State.

Has the Department of State ever turned any of your requests down?

If so, which countries have you been turned down for and what was their reasoning?

Response: At posts where ICE Visa Security Program (VSP) operations have been established, Department of State (DOS) and DHS personnel have established strong and productive partnerships that enhance the security of the visa process. In 2008, ICE VSP and DOS collaborated on VSP's site selection methodology and presented the joint findings to the Homeland Security Council. Additionally, DOS and ICE VSP released a 2008 cable to all posts highlighting the joint accomplishments of DOS and ICE VSP efforts overseas.

While ICE VSP's cooperation with DOS has been largely successful, ICE VSP has occasionally faced resistance from individual Chiefs or Deputy Chiefs of Mission towards the establishment of new Visa Security Units in certain locations. ICE VSP continues to coordinate site selections and visits to posts under consideration for ICE VSP deployment to explain the program's value.

56838.097

Question#:	24
Topic:	AIT
Hearing:	Intelligence Reform: The Lessons and Implications of the Christmas Day Attack
Primary:	The Honorable John Ensign
Committee:	HOMELAND SECURITY (SENATE)

Question: I know that the Department is looking to acquire Advanced Imaging Technologies. What is the Department doing to address the low-tech methods possibly being used by terrorists (i.e. placing explosives within their own body cavity)?

Response: The Transportation Security Administration (TSA) mitigates this threat through the expanded use of explosives trace detectors, allowing TSA to detect minute quantities of explosive trace particles present on the bodies of individuals who have handled or carry explosive materials. TSA works closely with the Department of Homeland Security's Science and Technology Directorate, as well as the National Laboratories under the Department of Energy, to develop new detection technologies.

56838.098

Opening Statement for Chairman Joseph I. Lieberman
Homeland Security and Governmental Affairs Committee
"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II"
January 26, 2010

The hearing will come to order. Good morning and welcome to this second in a series of hearings during which our Committee will examine how the intelligence reforms passed by Congress in the wake of the attack of 9-11 are working, and examine the reforms in light of recent terrorist attacks and the ongoing threat, and to determine what parts of what laws we passed earlier may perhaps need further reform so that we can fulfill our responsibility to protect the homeland security of the American people.

I want to just go back to last week's first in the series of hearings before I focus on this one and say that I very much appreciated the fact that all of our witnesses in last week's hearing – Director of National Intelligence Dennis Blair, Director of the National Counterterrorism Center Michael Leiter and Department of Homeland Security Secretary Janet Napolitano – acknowledged that mistakes were made with regard to the Christmas Day attack on the plane over Detroit, and all three of them offered to work with each other and with this Committee to make our existing multi-layered counterterrorist defenses quicker to react and harder to penetrate.

I thought Admiral Blair was especially forthright and I thank him for that. My guess is his forthrightness has probably brought him some criticism and made him the target of some displeasure, but it was definitely the right thing to do because he felt and he spoke in what he believed to be the national interest. It is self-evident that our homeland security intelligence and law enforcement agencies didn't work as we on this Committee, and as Governor Kean and Congressman Hamilton in their work post-9/11, would've wanted those agencies to work. The point is that unless the people in charge admit that, as our three witnesses did last week, the problems will never be fixed. And when they do deal with their shortcomings forthrightly, we have some hope that the problems will be fixed, and obviously whatever mistakes were made will not recur again.

I do want to say that one of the most troubling revelations at our hearing last week was that none of the three witnesses was consulted before the Christmas Day bomber was turned over to our criminal courts, rather than to the military where I believe he should have been held, since he was trained, equipped and directed to attack America by Al Qaeda.

Since our hearing last week, Osama bin Laden himself has boasted of Al Qaeda's sponsorship of the Christmas Day attack on America. And so, while Al Qaeda claims credit for this attack, Omar Farouk Abdulmutallab, whom I think we can fairly describe as a soldier of Al Qaeda, and obviously not an American citizen, now enjoys the Constitutional protections of an American citizen, including a lawyer who immediately counseled him to remain silent, even though he may have information that could protect the American people from another terrorist attack.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00292 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.099

To me this is outrageous – a kind of "Alice in Wonderland" turn of the world of common sense on its head.

And that is why yesterday Sen. Collins and I wrote to Attorney General Holder and Deputy National Security Advisor Brennan, urging them to immediately turn Abdulmutallab over to the Department of Defense, where he can be held as an enemy combatant, as a prisoner of war, which he is, acknowledging with some certainty and gratitude that this also means that he will be held and given rights far in excess of what the Geneva Convention requires enemy combatants or prisoners of war be given. Senator Collins and I and our committee are going to stand tough with this and other aspects of it to make sure that this mistake, the failure to consult with intelligence and homeland security officials before deciding how to handle Abdulmutallab and then the decision to turn him over to the civilian courts, is ever made again.

I do believe our homeland security intelligence gathering and analysis have remarkably improved since the attacks of 9-11, and that the sharing of intelligence, as we said last week, at all levels of government is vastly improved. This is due in no small measure to the work of two gentlemen who we're proud to have as our witnesses today: chairs of the 9-11 Commission, Governor Tom Kean and Congressman Lee Hamilton. The passage of the Intelligence Reform and Terrorism Prevention Act of 2004 has played a critical and extremely positive role in driving the changes that make the American people more secure today than we were on 9-11.

It's the work of these two gentlemen that leads us in part to refer to the Act I just referred to as the 9-11 Commission Act. That's the reason. The other reason is that it sounds a lot better than saying IRTPA, which is the acronym for the Act. The fact is that Act implemented most of the bipartisan recommendations of that Commission, and Governor Kean and Congressman Hamilton have been unique, not only in their bipartisan service on the Commission, but in continuing to track the implementation of their recommendations persistently over the last five years.

They are testifying before us today in their current capacity as co-chairs of the National Security Preparedness Group. I welcome both of you, and I thank you very much for your service.

Your Commission's recommendations were comprehensive, both in terms of long-term actions we can and should take to blunt the terrorists' appeal and to stop their ability to recruit, and also more short-term actions that we need to take to defend our nation against further attack.

One of the challenges revealed in our hearing last week was the overwhelming amount of information that is collected by our intelligence and law enforcement agencies for analysis. It has been estimated, as you gentlemen know, that the National Security Agency alone collects on a daily basis four times more information than is stored in the Library of Congress. Hard to imagine, but that's how much is being collected.

I know Governor Kean and Congressman Hamilton have been considering this challenge and I'll be interested to hear their thoughts on how we can better organize our intelligence

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00293 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.100

gathering and analysis efforts so that crucial information can be mined more quickly from the vast mountain of data we build. I mean, after 9-11, we were saying, correctly I believe, that the dots that we were collecting did not come together on the same board, as it were. I think now, thanks to your recommendations and the legislation that followed, the dots are coming together on the same board. But there's so many millions, billions of dots, the question is how do we see the patterns to help us act preemptively to stop attacks against our country?

Another question I'd like to explore in more detail with our witnesses relates to the authorities that we provided to the Director of National Intelligence and the National Counterterrorism Center in the 9/11 Commission Act. Bottom line question: do we need to give the DNI and the NCTC additional authorities, or do we need to push them harder to use the authorities they already have?

And again I know that the two of you have done some preliminary work on this and I look forward to the guidance that you can offer the Committee as we go forward with this series of hearings which is aimed at coming up with a report, a kind of status report, and perhaps recommendations for legislation or further executive action.

I cannot thank you enough for your unflagging efforts to secure our nation against terrorism, particularly Islamist terrorism – a rootless and shadowy enemy, driven by theological extremism and unbound by any sense of morality or respect for life. That's the challenge of our time and because of your extraordinary service, we are doing a lot better than we otherwise would have in meeting that challenge.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00294 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.101

Opening Statement of
Senator Susan M. Collins

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II"

Committee on Homeland Security and Governmental Affairs
January 26, 2010

★ ★ ★

Intelligence failures . . . . calls for reform . . . . lack of accountability . . . . testimony by Governor Kean and Congressman Hamilton. It sounds like the aftermath of the 2001 attacks all over again, but in fact, there are significant differences between now and then.

When our nation was attacked on the morning of September 11, 2001, our intelligence community was hampered by an organizational structure that undermined unity of effort. It was led by a Director that had little authority over its various elements and little incentive to focus beyond the mission of the Central Intelligence Agency. It was burdened with a culture that promoted parochial agency interests over the intelligence needs of a nation.

The Intelligence Reform and Terrorism Prevention Act of 2004 fundamentally changed our intelligence community. Working with the families of the victims and the 9/11 Commission, this Committee was able to pass the most substantial reforms of our intelligence agencies in more than 50 years.

In the five years since the Intelligence Reform Act became law, information sharing and collaboration among the 18 elements of the intelligence community have improved dramatically. And, in 2009 alone, the intelligence community, working with law enforcement and homeland security agencies, has helped detect and disrupt numerous terrorist attacks targeting our nation. Two of these successes were the arrests of David Headley and Najibullah Zazi in two separate terrorist conspiracies. Other successes also were made possible by the reforms this Committee spearheaded in 2004.

But, standing alone, a law cannot accomplish transformation. At the end of the day, even the most powerful laws are just words on paper. They rely on the President and leaders within the executive branch to produce reform. And, to fight the war on terrorism, the President, the Director of

56838.102

National Intelligence, the Secretary of State, and other leaders must use the laws passed by Congress to their fullest extent.

Unfortunately, the terrorist attack at Fort Hood and the failed Christmas Day plot are stark reminders of what can happen when those authorities are not used effectively.

Under the 2004 law, the DNI has the clear authority to "determine requirements and priorities." Yet, the DNI failed to respond to the growing threat that al Qaeda in the Arabian Peninsula posed to the United States and apparently failed to target sufficient resources at this threat.

The Intelligence Reform Act also provides ample authority "to ensure maximum availability of and access to intelligence information within the intelligence community." Yet, intelligence regarding the threat posed by Major Nidal Malik Hasan remained stove-piped at an FBI Joint Terrorism Task Force instead of being provided to officials within the Department of Defense who might have been able to act to prevent the Fort Hood attacks.

The law directs the DNI to "ensure the development of information technology systems that include . . . intelligence integration capabilities," yet intelligence that may have identified Abdulmutallab as a terrorist remained undiscovered in multiple intelligence community databases – disseminated, yet effectively unknown.

The law provides the Secretary of State with clear authority to revoke a visa "at any time, in [her] discretion," yet Abdulmutallab's visa remained valid when he boarded Flight 253 in Amsterdam. It remained valid despite the fact that the State Department had already decided to question him about his ties to extremists if he chose to *renew* his visa. How he could have been a threat to the United States in the *future* based on these extremist ties, but not a sufficient *current* threat to prudentially revoke his visa defies both logic and common sense.

And, finally, despite the President's authority to hold Abdulmutallab as an enemy belligerent and subject him to a thorough interrogation for intelligence purposes, the Department of Justice unilaterally decided to treat the foreign terrorist as a common criminal, advise him of the right to remain silent, and grant him a lawyer at the taxpayer's expense. Our nation's top intelligence officials were never even consulted on this decision.

56838.103

I direct attention to these failures not to assign blame at this stage of our inquiry, but to indicate that effective leadership may prevent similar mistakes in the future.

The President must empower his senior officials to use every authority available to them to defeat the terrorist threat.

These reforms do not require action by the Congress. They do not require a 60-day review to consider. They should be implemented now by the President. Nothing less than our security hangs in the balance.

56838.104

BIPARTISAN POLICY CENTER

Bipartisan Policy Center
Congressman Lee Hamilton and Governor Tom Kean
Testimony before the Senate Homeland Security Committee
January 26, 2010

Introduction

We are very happy to be back before you today. This committee's role in enactment of the historic Intelligence Reform and Terrorism Prevention Act was critical to the most substantial changes to the national security infrastructure since its creation in 1947. Senators Lieberman and Collins, as well as Congressman Hoekstra and Congresswoman Harman, went well above the call of duty to see to its enactment and that's something for which the country should be grateful.

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:

- Mr. Peter Bergen, CNN National Security Analyst and Author, Schwartz Senior Fellow at the New America Foundation
- 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

56838.105

- 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. House Homeland Security Staff Director
- The Honorable Richard L. Thornburgh, former U.S. Attorney General, Of Counsel at K&L Gates
- The Honorable Jim Turner, Former Congressman from Texas and Ranking Member of the U.S. House Homeland Security Committee, Arnold and Porter, LLP
- Mr. Lawrence Wright, New Yorker Columnist and Pulitzer Prize winning author of *The Looming Tower: Al Qaeda and the Road to 9/11*
- The Honorable E. Spencer Abraham, Former U.S. Secretary of Energy and U.S. Senator from Michigan, The Abraham Group

Over the course of 2009, our group met with Obama Administration and former senior officials from the Bush Administration, including:

- Director of National Intelligence, Admiral Dennis Blair (July 2009)
- CIA Director Leon Panetta (July 2009)
- Secretary of Homeland Security Janet Napolitano (July 2009)
- FBI Director Bob Mueller (September 2009)
- Former CIA Director Mike Hayden (September 2009)
- Former DNI Mike McConnell (September 2009)

We will also meet with Deputy National Security Adviser John Brennan this afternoon.

We believe the strength of our group will allow us to be a voice on national security issues and a resource to you and the executive branch. First and foremost, we are here to help play a constructive role in support of your work.

Recently the 5 year anniversary of the Intelligence Reform and Terrorism Prevention Act passed and that makes it an appropriate time for us to consider how well this has worked and whether additional changes need to be made. At the Bipartisan Policy Center, our National Security Preparedness Group has been studying the implementation of the 9/11 Commission's recommendations, especially the state of intelligence reform, and new threats to our national security.

We look forward to working with you, and benefiting from the work of this committee, as our study continues.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00299 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.106

We should state at the outset that the events that transpired on Christmas give us the opportunity to make two important points.

First, the threat from al Qaeda and radical Islam remains strong. Al-Qaeda's core is still active, individuals are still being radicalized in Western countries and motivated to commit violence, and homegrown lone actors are still a risk. As our colleague Bruce Hoffman observed, "al Qaeda is on the march, not on the run." We have been concerned that our sense of urgency on terrorism has been low. We must reject complacency and recognize we still face a serious threat from organizations like Al-Qaeda. This is not a reason for panic but for a concerted, comprehensive effort.

Second, as we see that the determination of the terrorist to attack the homeland remains unabated, it reminds us of the need for establishing a Director of National Intelligence and a National Counter Terrorism Center in the first place. At their core, the problems evident on September 11, 2001, were about the failures and obstacles to sharing information among the federal partners charged with protecting the country and that there was no one in the federal government charged with fusing together intelligence derived from multiple foreign and domestic sources. The DNI has been charged with breaking down bureaucratic, cultural, technological, and policy barriers to the sharing of information among federal agencies and the NCTC has been successful in a number of incidents in helping thwart potential terrorist attacks.

We need to support these entities and build them into enduring institutions. It is imperative that the DNI and the NCTC to be successful in the vital missions they have been asked to undertake for the country.

Effectiveness of the DNI

We are very pleased your committee has initiated this series of hearings to study how well intelligence reform has been implemented. This is the kind of congressional oversight the 9/11 Commission called for and we welcome your efforts to scrutinize the activities of our national security system.

There has been a debate within the intelligence community on the state of intelligence reform and the effectiveness of the DNI. The DNI has been hobbled by endless disputes over its size, mission, and authority. We too are concerned about the expanding growth and bureaucracy of the DNI and we urge vigorous reevaluation of all its functions to assure its leanness. But such a review must

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00300 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.107

occur with the recognition that the Congress and the President gave the DNI a massive to do list in the wake of the intelligence failures of 9/11 and weapons of mass destruction in Iraq. This to do list includes:

- Solving systemic and longstanding information-sharing issues among Intelligence Community entities, especially to break down the "wall" between foreign and "domestic" intelligence, and to create an architecture to enable such sharing;
- Serving as the President's Principal Intelligence Advisor;
- Developing a national intelligence budget across all intelligence agencies;
- Overseeing billions of dollars of intelligence community acquisitions;
- Improving the quality of intelligence analysis, especially to guard against "group-think," and to manage an intelligence process that is inclusive of a variety of view points;
- Strengthening management across the Intelligence Community;
- Advancing and using the latest science and championing new research and development efforts;
- Creating a work force within the Office of the DNI with the right people to execute these important functions;
- Facilitating a "culture change" within the Community by establishing a joint duty system, modeled on DoD's Goldwater-Nichols, to enable personnel to rotate assignments within the intelligence community;
- Bringing a mission focus to the IC by creating a group of Mission Managers "responsible for all aspects of the intelligence process to those issues" and leading centers like National Counter Terrorism Center and National Counterproliferation Center.

It is not enough to say simply that the DNI bureaucracy should be reduced. We need to take a fresh look at how the DNI has performed on these essential tasks, clarify the mission of the DNI, and then seek to adjust accordingly.

In recent months as we have studied the effectiveness of the DNI we have come to some preliminary conclusions. We have more work to do but we believe that the DNI has achieved a meaningful measure of success in its first years – that has made it worth the inevitable turmoil – but is a work in progress closer to the beginning of reform than the end. Some of the successes in the last five years include progress on information-sharing, a joint-duty program, and despite the failures evident in the Christmas attack, the National Counter Terrorism Center. Since September 11, 2001, the NCTC and other government agencies have repeatedly connected the dots and shared information necessary to defeat terrorist

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00301 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.108

attacks. Improvements have clearly been made although that sharing is not as prompt and seamless as it should be.

But many of the successes of the DNI have been heavily dependent on key personalities within the executive branch. We want to continue to look closely at the authorities of the DNI to make sure he has the authority to do his work, but it is our sense that the success of the DNI in the short term will not rise or fall on whether we make additional statutory adjustments to IRTPA.

To be sure, we believe there are some ambiguities in the law. Section 1018, the passage designed to ensure the chain of command in departments and agencies will not be abrogated, would certainly be in that category, although we understand that some of the problems resulting from this section were at least partially remedied in revisions to Executive Order 12333. Some ambiguities were the product of legislative compromise which is a fact of life in our political system.

Nonetheless, there are still ambiguities and they can contribute to mission confusion and lack of clarity about lanes in the road. This is perhaps the greatest challenge facing the DNI. Is the DNI a strong leader of the intelligence community empowered to lead the IC as an enterprise? Or is the DNI a mere coordinator, a convening authority charged with helping facilitate common inter-intelligence agency agreement? The lack of settled clarity on its mission invites a host of other criticisms, including that the ODNI is too large, too intrusive, and too operational.

The burden is on the President to be clear on who is in charge of the Intelligence Community and where final authority lies on budget, personnel, and other matters. In our estimation, we need a strong DNI who is a leader of the intelligence community. The DNI must be the person who drives inter-agency coordination and integration. At the same time, the DNI's authorities must be exercised with discretion and consideration of the priorities and sensitivities of other intelligence agencies. But the President's leadership is crucial and must be continuing or we run the risk of mission confusion and decrease the prospect of long and lasting reform that was recommended after September 11, 2001. The DNI's ability to lead the Intelligence Community depends on the President defining is role and giving him the power and authority to act.

Lessons from Christmas Attack

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00302 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.109

Much has been said on the lessons from the Christmas attack. We would like to highlight two issues.

First, the greatest single challenge that arises from this incident in our view is the urgent need to strengthen the analytic process.

As President Obama said, there was a failure to connect the dots. With more rigorous analysis, we might have been able to connect disparate pieces of information that might have foretold of the Christmas plot. We are pleased the President asked the DNI to look at this issue. The DNI was charged by the Congress to ensure the highest analytical standards within the Intelligence Community. The DNI is properly situated within that Community to assume a leadership role in applying more rigorous standards to analytical tradecraft. We hope the DNI will take a look at the incentives structure within the IC to reward analysts so we might recruit and retain the best people. We especially have in mind places in the intelligence community where analysts take a back seat to operators. We need to increase the prominence of the analyst which will lead to a lifting of standards across the intelligence community. Congress should also support these entities by giving the DNI and the NCTC the resources they need and the ability to recruit and keep the best people.

Another part of improving analysis is judging sources of potential attacks properly. As the President's review has shown, we had a "strategic sense" that Al Qaeda in the Arabian Peninsula was becoming a threat, but "we didn't know they had progressed to the point of actually launching individuals here." We collect a tremendous amount of intelligence and we need the very best people not only sorting through it for tactical details, but in a strategic sense asking where the next attack will come from.

The principal challenge to improved analysis is that the Intelligence Community is awash with data. In an age when we are collecting more information than ever before, the real challenge is how do you understand, manage, and integrate vast amount of information. The DNI needs to develop ways of dealing with intelligence information overload. At the same time, we need to do a better job of pushing information to the right people within the Intelligence Community. We welcome President Obama's order to distribute intelligence reports more quickly and widely. We need better management of the data and 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

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00303 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.110

information together and it must be properly placed instantaneously so better analysis can occur.

A second lesson from the Christmas attacks is that it reminds of the importance of eliminating terrorist sanctuaries. Finding that our attackers on 9/11 benefited from the time, space, and command structure afforded in Afghanistan, the 9/11 Commission placed great emphasis on identifying and prioritizing actual or potential terrorist sanctuaries. We recommended strategies employing all elements of national power to keep terrorists insecure and on the run. We're fortunate that the attack on Christmas emanating from Yemen did not succeed and this episode reminds us of the need to identify other potential sanctuaries. As our colleague Bruce Hoffman observed: "Al Qaeda is aggressively seeking out, destabilizing and exploiting failed states and other areas of lawlessness . . . and over the past year has increased its activities in places such as Pakistan, Algeria, the Sahel, Somalia, and of course Yemen." The U.S. should take a fresh look at these areas and deepen our commitment to ensuring al Qaeda cannot exploit those territories.

Privacy and Civil Liberties

The balance between security and liberty will always be a part of the struggle against terrorism. America must not sacrifice one for the other and must be in the business of protecting freedom and liberty as well as fighting terrorism. Following the 9/11 Commission recommendations, the Bush Administration created a Privacy and Civil Liberties Oversight Board to advise the executive branch and oversee government efforts to defend civil liberties. The board was staffed and became operational in 2006. In 2007, Congress restructured the Board as an independent agency outside the White House. Despite early accusations of undue delay and inadequate funding, the Board held numerous sessions with national security and homeland security advisers, the attorney general, and the FBI director, among others, on terrorist surveillance and other issues arising from intelligence collection.

However, the Board has been dormant since that time. With massive capacity to develop data on individuals, the Board has to be the champion of seeing that collection capabilities do not intrude into privacy and civil liberties. We continue to believe that the Board provides critical functions and we urge President Obama

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00304 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.111

to reconstitute it, quickly appoint its Members, and allow them full access to the information and the authority to perform to perform this essential function.

Congressional Oversight

The 9/11 Commission also placed great importance on rigorous congressional oversight. This recommendation helped precipitate the creation of a House Homeland Security Committee and a Senate Homeland Security and Governmental Affairs Committee. However, enduring fractured and overlapping committee jurisdictions on both sides of the hill have left Congressional oversight in a unsatisfactory state. DHS entities still report to dozens of separate committees hundreds of times per year, which constitutes a serious drain of time and resources for senior DHS officials. Further, the jurisdictional melee among the scores of Congressional committees has led to conflicting and contradictory tasks and mandates for DHS. Without taking serious action, we fear this unworkable system could make the country less safe.

The 9/11 Commission also called congressional oversight over intelligence dysfunctional. We made recommendations to strengthen the oversight committees which were not accepted by the Congress though some progress has been made. Today we want to emphasize the enormous importance we attach to rigorous oversight of the intelligence community. Congressional oversight can help ensure the intelligence community is operating effectively and help resolve disputes about conflicting roles and missions. We urge the Congress to take action to strengthen the oversight capabilities of the intelligence committees.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00305 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.112

Post-Hearing Questions for the Record
Submitted to the Honorable Thomas H. Kean
and the Honorable Lee H. Hamilton
From Senator Claire McCaskill

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 26, 2010

1. **In your testimony, you recommended to the Committee that we need to be giving DNI additional support to do their job more effectively. Can you expand upon this recommendation? How is DNI not currently being supported? Is this an issue of lack of funding? Are there specific examples of a lack of support? What specifically can Congress be doing to provide DNI with additional support?**

   The Director of National Intelligence has a difficult job in managing an intelligence community spread out over many departments and agencies. Congress, in their oversight capacity, can play an important role in helping reinforce the spirit of intelligence reform, especially that the IC needs to act more like a joint enterprise. For example, hearings designed to encourage further cooperation and jointness, like the hearings conducted by the Senate Homeland Security Committee, can play an important role in surfacing issues that need higher level attention.

2. **During your testimony before the Committee, you stated that the Intelligence Community needs to raise the prominence of analysts and Congress needs to support these needs by giving DNI and NCTC the resources to do so. What led you to the conclusion that analysts do not have the prominence required in their communities? What can Congress be doing to ensure that DNI is able to keep and recruit the best analysts?**

   One of the lessons from the after-action reports regarding the December 2009 attempt was that the intelligence community collects a tremendous amount of information. As President Obama said with regard to this incident, there was a failure to connect the dots. With more rigorous analysis, we might have been able to connect disparate pieces of information that might have foretold of the plot. The DNI was charged by the Congress to ensure the highest analytical standards within the Intelligence Community and is properly situated within that Community to assume a leadership role in applying more rigorous standards to analytical tradecraft. Our statement in January noted that analysts take a "back seat to operators." We based this on our observations of the intelligence community and membership on a variety of other panels and advisory groups on which we have served. One way Congress can help the DNI is able to keep and recruit the best analysts is to ensure the DNI and other intelligence agencies have the funding, are empowered to create the right incentives structures, are continuing to implement programs to ensure rigorous analytical tradecraft.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00306 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.113

3. **There are several references in your testimony indicating that the 9/11 Commission's most difficult and important recommendation that has not been implemented is the strengthening of Congressional oversight of the Intelligence Community. You stated that there are too many overlapping Congressional committees of jurisdiction that absorb time and lead to distortion and contradictory congressional direction. I share Senator Lieberman's sentiment that we should revisit this recommendation. What is your recommendation for moving forward especially given the sensitive congressional jurisdiction challenges that lay ahead?**

   We have stated on many occasions that changing congressional committee jurisdiction is one of the hardest things to do in Washington. As you mention, this is a delicate matter that would take a tremendous amount of effort. We believe that most reform efforts succeed from within, when Members of Congress see the problem and advocate change. We are willing to continue to play an outside advocacy role and would welcome the opportunity to discuss this matter further with you.

4. **DHS currently only uses the selectee and the no-fly list to screen passengers for purposes of secondary screening. They do not screen the Terrorist Identity Datamart Environment (TIDE) and Terrorist Screening Database (TSDB) lists prior to flight departure. Having access to all of the information in my mind would be the ideal situation. Do you recommend allowing DHS to access the TIDE and TSDB lists? In your view would allowing DHS to secondarily screen a passenger on the TSDB be appropriate? What would be the logistical or privacy implications of such a decision?**

   The 9/11 Commission highlighted the importance taking aggressive measures to limit terrorist travel and the ideas you mention are certainly consistent with our recommendations, especially that TSA should utilize a larger set of watchlists maintained by the federal government. Ensuring that the officials controlling entry onto airplanes have all the information they need to make a decision strikes us as a necessity. You rightly identify operational and privacy considerations. These are very complex issues that need to be sorted through with the advice of a Civil Liberties Board, a 9/11 Commission recommendation that needs to be implemented. While we need to strive for security and protection of civil liberties, it makes sense to us that we need to empower individuals charged with safeguarding our security with the information they need to do the job.

5. **There is something that also must be taken under consideration in future screening concepts of operation. If we flagged an individual too late, as we did in the Abdulmutallab case, and the flight departed with a questionable individual on board, what recommendation would you provide with regards to notifying and advising the crew of the particular threat of the passenger while in-fight? Ultimately, we want to be able to catch these individuals before they get on the**

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00307 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.114

plane, but if we don't I want to make sure there is proper training and protocols in place to counter the threat with and without a Federal Air Marshall. Would you recommend a requirement to notify the crew of the flight if there is concern about a passenger, such as in the case of the alleged 12/25 bomber? In this case, given that Abdulmutallab spent 20 minutes in the bathroom prior to igniting the explosive, we might have been able to prevent him from even attempting the act.

Yes, we agree that is sensible that if there is a dangerous individual aboard a plane in flight, the potential threat should be relayed to the crew. While we would want to study this issue further to ensure all dimensions of this scenario have been considered, on its face this seems like the right thing to do.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00308 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.115

Opening Statement for Chairman Joseph Lieberman
"The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening"
Homeland Security and Governmental Affairs Committee
March 10, 2010
As Prepared for Delivery

Good morning, and welcome to this Committee's third hearing in a series that Senator Collins and I have begun to examine the extensive reforms made to our intelligence systems both after September11, 2001, but particularly at the five year point from the enactment of the 9/11 Commission reforms. Our goals here are to review how we're doing, to identify weaknesses that remain in the system, and make recommendations for administrative reform or legislation that are needed to correct those weaknesses. Of course, these hearings have taken on added significance in the aftermath of the Christmas Day terrorist attack in which Umar Farouk Abdulmutallab unfortunately exposed some serious weaknesses in our nation's homeland defenses.

The last two hearings that we've done in this series gave us a broad overview of the human mistakes and the structural shortcomings that contributed to the Christmas Day attack. Today, we will look at two of the most important components of our government's efforts to deny terrorists the ability to travel to the United States, and that is the creation and use of terrorism watchlists and the passenger pre-screening mechanisms that use these lists to identify potentially dangerous individuals and, if in fact we determine they are such, stop them from getting on airplanes coming to the United States.

On Christmas Day our government was unable to pull together all the intelligence in its possession to stop Abdulmutallab before he got on that plane. This was not a failure to collect information and, unlike the missteps leading up to 9/11, it was not a failure to share it: We knew that Abdulmutallab's father had concerns about his son's growing extremism and presence in Yemen. We had intelligence that there was a Nigerian—unnamed, unidentified, but a Nigerian nonetheless--training in Yemen with Al Qaeda in the Arabian Peninsula. We heard separately of plans for a Christmas-time attack on the United States. And, again separately, we knew of a reported telephone intercept that identified a man named Umar Farouk, without his last name, as a terrorist. All those dots were on the same table but our government was unable to connect them – to separate this information out of the enormous mass of information our government collects and shares so that this terrorist could be stopped before he acted. We were just plain lucky that the device he had on him did not effectively explode on that plane.

In our first hearing, National Counterterrorism Center Director Mike Leiter acknowledged that the Center's information collection and sharing systems need to be smarter. And I would add, in an era when Google, for instance, can aggregate information for anybody who goes on Google from scores of websites and databases throughout the world very quickly, it is unacceptable that NCTC does not have the same ability to search and aggregate information across our government's intelligence databases.

I think we also need automated mechanisms to connect disparate data points 24/7, 365 days a year and flag potential threats for analysts to examine. These systems are widely used in the private sector, and need to be adopted by our intelligence community ASAP.

The Abdulmutallab case also exposed weaknesses in our watchlisting system. Our intelligence agencies obviously need to view some tips with skepticism as informants may be motivated by spite or rivalry. But, most are not, and it is just unacceptable that Abdulmutallab's father, a respected business leader in Nigeria, was not

56838.116

considered a credible enough source for his information to put his son on the watchlist without corroborating evidence. I hope to hear from our witnesses today how the watchlisting process has been modified to ensure that this kind of error will not be made again.

Another watchlisting problem concerns the screening of individuals on the watchlist who are not U.S. citizens or permanent residents. We are historically one of the most welcoming countries in the world to visitors. But travel to the United States is a privilege, not a right. In my opinion, if the government concludes that there is any reason to believe someone may have ties to terrorist activities, that person should be required to undergo secondary physical screening before being allowed to board a plane bound for the United States of America.

Finally, we need to dramatically expand our ability to pre-screen travelers, both internationally and domestically. Right now, the government only begins to receive important identifying information about international travelers when they check in for their flight. In fact, most of this information is conveyed to the Department of Homeland Security only when an airplane's doors are about to close, which makes it practically impossible for DHS to fully vet passengers before a plane takes off. That was the case on Christmas Day and it argues loudly that we start in-depth vetting well in advance of a passenger's arrival at the airport, using modern information technology and data gathering. We need to ensure that DHS has the identifying information it needs about international passengers at least 24 hours before departure and that it fully implements Secure Flight to ensure that all passengers on all flights are systematically checked against the terrorism watchlists.

This hearing is an important opportunity to examine the next steps we need to take to continue to strengthen these watchlists and prescreening systems that have been established after 9/11 and particularly after the passage of the 9/11 legislation. We're doing much better at this than we did after 9/11, but what the Christmas Day bombing attempt shows is that we have to do better yet to ensure that the next Abdulmutallab is not allowed to get on a plane to the United States.

We've got a very good group of witnesses before the Committee today. I want to say to you that I think you have some of the hardest jobs in the United States Government and though you are therefore subjected to our criticism periodically I want to thank you for your commitment and service to our country.

-30-

56838.117

Opening Statement of
Senator Susan M. Collins

"The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening"

Committee on Homeland Security and Governmental Affairs
March 10, 2010

★ ★ ★

Today's hearing focuses on two fundamental questions: why was the Christmas Day bomber, Umar Farouk Abdulmutallab, allowed to travel to the United States, and why wasn't his name included on the terrorist watchlist?

We know that Abdulmutallab's father had informed the American Embassy in Nigeria of his Islamist extremist connections in Yemen more than a month before he boarded the flight to Detroit. We also know that his name was included in the broadest terrorist database, known as TIDE. But despite this alarming information, the system failed to bar Abdulmutallab from boarding Flight 253 to America.

This is a case of missed opportunities.

From my perspective, the State Department clearly had sufficient information to revoke Abdulmutallab's visa. State Department officials already had decided to question Abdulmutallab about his ties to extremists if he chose to *renew* his visa. How he could have been a threat to the United States in the *future* based on his extremist ties, but not a sufficient *current* threat to suspend his visa defies both logic and common sense. Had the State Department taken this action, it would have prevented him from traveling to the United States. A missed opportunity.

Another missed opportunity occurred in Amsterdam, where Abdulmutallab's flight originated. This airport is one of only nine foreign airports where a small number of U.S. immigration advisory officers are stationed. These officers can ask an airline not to board a passenger who will be prohibited from entering our country upon arrival. They receive a list of passengers of concern, including those whose visas have been revoked or flagged by the State Department. This was another missed opportunity to stop Abdulmutallab.

Recently, the Department of Homeland Security has expanded its efforts to identify individuals who have revoked visas or who are on the

56838.118

State Department's visa watch list before they board airplanes overseas, rather than waiting until they have already arrived at U.S. airports. I would like to know how successful these programs are at identifying high-risk travelers.

Another missed opportunity to stop Abdulmutallab occurred at the NCTC. The President has stated that there was ample intelligence on Abdulmutallab to warrant his inclusion on the No Fly list. Yet that did not occur, even after his father's warning. It did not occur because other streams of intelligence were not connected until it was too late. Why did the Intelligence Community fail to analyze all available information relating to Abdulmutallab?

Some intelligence experts point to outmoded systems as a factor. Despite vast improvements in information sharing, our Intelligence Community continues to rely on internal systems that are relics from the days before the Intelligence Reform and Terrorism Prevention Act of 2004. These outdated systems do not effectively surface intelligence information so that analysts and security officials can identify threats in real-time.

I would like to know the Administration's plans for upgrading systems to allow for more effective searching of terrorist information. For starters, identifying individuals in the terrorist databases who have valid U.S. visas should not be a complicated task.

We also must examine how we can better identify individuals who should be on watchlists for additional screening at airports. For example, we know that Abdulmutallab was identified for additional screening once he arrived in Detroit while his flight was in the air.

Why wasn't that same information used to identify him earlier, before he boarded his flight? Another missed opportunity. As this case demonstrates, waiting until a suspected terrorist arrives in the U.S. to conduct additional screening is waiting too long.

We must continue to strengthen our watchlisting and screening systems. Unless these systems work effectively, we will not be able to prevent terrorists' from traveling to our nation.

# # #

56838.119

Statement of Senator Thomas R. Carper

Committee on Homeland Security and Governmental Affairs

March 10, 2010

The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Thank you, Mr. Chairman.

I'd like to first begin by thanking each of our witnesses today for taking the time to join us as we explore how we should address the shortcomings that allowed Umar Farouk Abdulmutalib to board an airplane on December 25, 2009.

As we all know, it is extremely difficult to be right 100 percent of the time when it comes to these matters. And as Secretary Napolitano said during her last appearance before this committee, 'there is not just one silver bullet' we can deploy to stop terrorists from trying to enter our country and do us harm. The battle we're engaged in is not one we can win with guns or tanks alone. It's probably not one that we can win solely with some of the new screening technology that we're talking about deploying in more airports. We'll need to get smarter, adapt as those who wish to do us harm change their tactics and continue the efforts this committee embarked on after 9/11 to improve our intelligence operations and information sharing.

Effective intelligence analysis involves both the use of technology and skilled people to identify threats and know which ones to act on. Our security systems need to be more agile and our intelligence officers, who are on the front lines every day, must be encouraged to share information with each other. We also need to look closely at what our friends around the world are doing to police their airports and pre-screen passengers boarding their airplanes.

In closing, I'd also would like to express the urgency for this Congress to confirm in a timely manner President Obama's nominee, Major General Robert A. Harding, to lead the Transportation Security Administration. This position has been vacant for over a year now and is too important to our national security to be without a permanent Assistant Secretary. I look forward to working with my colleagues to make sure that it is filled as soon as possible.

56838.120

Committee on Homeland Security and Governmental Affairs

United States Senate

March 10, 2010

The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Statement for the Record

of

Mr. Russell Travers

Deputy Director for Information Sharing and Knowledge Development

National Counterterrorism Center

Statement for the Record

March 10, 2010

Committee on Homeland Security and Governmental Affairs

The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee: Thank you for your invitation to appear before the committee to discuss terrorist screening procedures in light of the attempted terrorist attack on Christmas Day.

It is my privilege to be accompanied by my colleagues from the Federal Bureau of Investigation and the Department of Homeland Security.

Watchlisting Issues Associated with the Incident

Umar Farouk Abdulmutallab was not watchlisted. This statement will explain the reasons why – addressing the post 9/11 changes in U.S.Government watchlisting practices, the associated standards that were adopted by the U.S. Government, and the application of those standards to the case of Umar Farouk Abdulmutallab. It will also address lessons learned as we strive to improve the Intelligence Community's ability to support watchlisting and screening.

- Before the September 11 terrorist attacks, intelligence databases and watchlisting systems were badly disjointed. They were neither interoperable nor broadly accessible and, as a result, two of the hijackers – although known to parts of the U.S. Government in late-1999, were not watchlisted until late-August 2001.

- To fix that systemic problem, the U.S. Government implemented Homeland Security Presidential Directive-6 (HSPD-6) in the Fall of 2003. Under the construct of HSPD-6, all collectors would provide information on known and suspected terrorists (except purely domestic terrorists) to NCTC which maintains a TOP SECRET database called the Terrorist Identities Datamart Environment (TIDE). Every night a FOR OFFICIAL USE ONLY extract of TIDE is provided to the Terrorist Screening Center (TSC) to support all U.S. Government screening operations.

    - The determination of what information is passed from TIDE to the TSC is governed by the "reasonable suspicion" standard which describes the minimum derogatory information for inclusion on the consolidated watchlist.

    - That criteria, approved by the Deputies Committee in the Fall of 2008, notes that "individuals described as militants, extremists, jihadists, etc should not be nominated without particularized derogatory information."

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00315 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.122

- The implementing instructions further state "those who only associate with known or suspected terrorists, but have done nothing to support terrorism" are ineligible for the No Fly List (NFL) or Selectee List (SL).

Mr. Abdulmutallab was in TIDE, but his name was not passed to the TSC for watchlisting. This was due to two factors:

- The TIDE record that existed on Mr. Abdulmutallab was based primarily on information provided to the U.S. Embassy in Abuja, Nigeria on November 20, 2009. The cable included one general sentence of derogatory information related to his possible association with Yemeni-based extremists. The entire watchlisting community agrees that the level of derogatory information contained in the November 20, 2009 cable did not meet the minimum standard highlighted above and was insufficient for any level of watchlisting---much less either the No Fly List or Selectee lists.
    - As a result, Mr. Abdulmutallab was entered into TIDE November 23, 2009, but his name was not passed to the TSC for watchlisting. Additional biographic information was added to the record over the course of the next week, but no additional derogatory information was provided.
    - In order to provide some context, on any given day hundreds of other names are added to TIDE and virtually all of them would have far more alerting derogatory information than Mr. Abdulmutallab's record.
- While the November 20, 2009 cable formed the basis for the TIDE record and the watchlisting status as of December 25, 2009, we learned after the incident of additional reporting that---had it been linked to the November 20, 2009 cable---could have supported a watchlisting nomination.
    - Had this information been linked to Mr. Abdulmutallab's record, his name undoubtedly would have been entered on the visa screening "lookout" list and the border inspection list.
    - Whether Mr. Abdulmutallab would have been placed on either the No Fly List or the Selectee List would have been determined by the strength of the analytic judgment.
    - It is important to note that the linkage of these pieces of information appears far more apparent in hindsight than it would have at the time. The reporting existed in daily intelligence holdings that number well into the thousands. Partial names and different spellings complicated the linkage. To be sure, the Intelligence Community continues its efforts to improve performance, but linking two pieces of fragmentary information can be a very difficult analytic problem. The two cables existed largely "in the noise" and there was simply nothing particularly alerting about either "dot."

Lessons Learned

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00316 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.123

- First of all, it is necessary to dispel two myths:
    - This situation doesn't implicate the HSPD-6 watchlisting architecture. The National Counterterrorism Center continues to believe it is fundamentally sound.
    - This incident does not raise major information sharing issues. The key derogatory information was widely shared across the U.S. Counterterrorism Community. The "dots" simply were not connected.
- The incident does highlight the following issues:
    - The U.S. Government needs to look at overall standards---those required to get on watchlists in general, and the No Fly List and Selectee List in particular.
    - The U.S. Government needs to improve its overall ability to piece together partial, fragmentary information from multiple collectors. This requirement gets beyond watchlisting support, and is a very complicated challenge involving both numbers of analysts and the use of technology to correlate vast amounts of information housed in multiple agencies and systems.

The men and women of the National Counterterrorism Center and the Intelligence Community are committed to fighting terrorism at home and abroad, and will seek every opportunity to better our analytical tradecraft, more aggressively pursue those that plan and perpetrate acts of terrorism, and effectively enhance the criteria used to keep known or suspected terrorists out of the United States.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00317 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.124

Statement of
Timothy J. Healy
Director
Terrorist Screening Center
Federal Bureau of Investigation

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

At a Hearing Entitled
"The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening"

March 10, 2010

Good morning Chairman Lieberman, Ranking Member Collins and members of the Committee. Thank you for the opportunity to discuss the Terrorist Screening Center (TSC) and its role in the interagency watchlisting process.

The attempted terrorist attack on Northwest Flight 253 on December 25, 2009, highlights the ever-present terrorist threat to our homeland. Over the past seven years, the TSC has played a vital role in the fight against terrorism by integrating terrorist information from the law enforcement and intelligence communities into a single database known as the Terrorist Screening Database (TSDB), which populates the various terrorist screening systems used by the Government. Following the Christmas Day attempted attack intense scrutiny has been placed on the requirements to nominate individuals to the watchlist and particularly to the No Fly and Selectee lists, which are subsets of the TSDB. These requirements, or standards, have evolved over time based on the experience of the watchlisting community and the issuance of additional Presidential Directives. Throughout this process, the TSC has remained committed to protecting the American public from terrorist threats while simultaneously protecting privacy and safeguarding civil liberties. As our efforts continue to evolve in response to new threats and intelligence, your support provides us with the tools necessary to continue our mission. Let me begin by telling you about the Terrorist Watchlisting process and how this process related to Umar Farouk Abdulmutallab.

Terrorist Nomination Process

The TSDB, commonly referred to as the Terrorist Watchlist, contains both international and domestic terrorist information. The procedure for submitting information on individuals for inclusion on the Terrorist Watchlist is referred to as the nomination process. The nomination process is the most fundamental and singularly important step in the watchlisting process. It is through this process that individuals are added to the Terrorist Watchlist. Nominations originate from credible information developed by our intelligence and law enforcement partners. These

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00318 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.125

intelligence and law enforcement agencies are referred to as Originators in the watchlisting community because it is through their work that nominations are developed. Federal departments and agencies submit nominations of known or suspected international terrorists to the NCTC for inclusion in NCTC's Terrorist Identities Datamart Environment (TIDE) database, which is the source of all international terrorist identifier information in the TSDB. NCTC reviews TIDE entries and nominates entries to TSC that include sufficient biographical or biometric identifiers and supporting derogatory information that meet the watchlisting standard described below. Similarly, the FBI collects, stores, and forwards to the TSC information relating to domestic terrorists that may not have connections to international terrorism.

When submitting a nomination to NCTC, an Originator may, but is under no obligation to, submit recommendations regarding specific screening systems the nomination should be exported to (e.g., inclusion on either No Fly or Selectee list). If an Originator submits a nomination without a recommendation, NCTC may make an appropriate recommendation based on the totality of associated information. Recommendations made by NCTC will be passed to the TSC for final disposition.

TSC accepts nominations when they satisfy two requirements. First, the biographic information associated with a nomination must contain sufficient identifying data so that a person being screened can be matched to or disassociated from a watchlisted terrorist. Second, the facts and circumstances pertaining to the nomination must meet the reasonable suspicion standard of review established by terrorist screening Presidential Directives. Reasonable suspicion requires articulable facts which, taken together with rational inferences, reasonably warrant the determination that an individual "is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of or related to terrorism and terrorist activities." The reasonable suspicion standard is based on the totality of the circumstances in order to account for the sometimes fragmentary nature of terrorist information. Due weight must be given to the reasonable inferences that a person can draw from the available facts. Mere guesses or inarticulate "hunches" are not enough to constitute reasonable suspicion. A TSC interagency group composed of members from the intelligence and law enforcement communities issued clarifying guidance to the watchlisting community in February 2009.

TSC makes the final decision on whether a person meets the minimum requirements for inclusion into TSDB as a known or suspected terrorist and which screening systems will receive the information about that known or suspected terrorist. It is not uncommon for a nomination to have multiple recommendations throughout the watchlisting process. In the end, however, TSC works with NCTC and the Originators to ensure a nomination is exported to as many screening systems as the nomination information supports.

The watchlisting and nomination process can best be described as a watchlisting enterprise because it requires constant collaboration between the Originators, NCTC, and TSC. NCTC relies upon the information provided by the intelligence and law enforcement community, TSC relies upon NCTC to analyze and provide accurate and credible information, and the screening community relies upon TSC to manage that information and to efficiently export it to their screening systems.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00319 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.126

Export to Supported Systems

Once a known or suspected terrorist is identified and included in the TSDB, TSC ensures the timely dissemination of the terrorist identity data to our screening partners. The utility of the watchlisting process is greatest when the information is efficiently disseminated to those who need it the most. The TSC's subject matter experts, who are composed of experienced analysts and designated agency representatives, review nominations to determine whether they meet the criteria for inclusion in the screening systems supported by the TSDB. The four major U.S. Government systems supported by the TSDB are: Department of State's Consular Lookout and Support System (CLASS) for passport and visa screening; Department of Homeland Security's TECS system for border and port of entry screening; the No Fly and Selectee lists used by the Transportation Security Administration for air passenger screening; and the FBI's National Crime and Information Center's Known or Suspected Terrorist File (formerly known as the Violent Gang/Terrorist Organization File (VGTOF)) for domestic law enforcement screening. The criteria for inclusion in each of these systems are tailored to the mission, legal authorities, and information technology requirements of the department or agency that maintains the system. Accordingly, each of these systems contains a different subset of data from TSDB.

The TSDB exports most pertinent to Umar Farouk Abdulmutallab – CLASS, TECS, and the No Fly and Selectee lists– are discussed below.

CLASS

CLASS is a database administered by the Department of State's Bureau of Consular Affairs and is used by consular officers abroad to screen visa applicants for travel to the United States. CLASS accepts nearly all records from the TSDB because minimal biographic information is necessary for visa screening. In other words, given where (overseas) and when (well in advance of travel to the U.S.), the Government has time to work through what can sometimes be less than complete biographical information – time that might not otherwise be feasible in other screening situations like a routine traffic stop or a busy overseas airport where the presence of U.S. officials is often minimal. The Department of State also uses a screening system known as CLASS-PASSPORT to screen applications for U.S. passports.

The TSC aids the Department of State in identifying known or suspected terrorists through two different processes. The first is the Security Advisory Opinion (SAO) process, whereby individuals that are watchlisted could be identified at the time of their visa application to visit the United States. When consular officers process visa applications, checks are run in CLASS to determine whether any derogatory information exists to warrant a visa denial. If it is determined that the visa applicant is a possible match to an individual on the Terrorist Watchlist, the consular officer requests an SAO. The SAO request is forwarded to the TSC, where the Department of State's subject matter experts at the TSC review the associated TSDB and TIDE records to determine whether the visa applicant is in fact the same watchlisted individual. The TSC's only role in this process is to determine if the individual applying for the visa is the same individual on the Terrorist Watchlist. In the case of a positive match, the TSC forwards the information to the Department of State's Visa Office, in the Bureau of Consular Affairs, to prepare an SAO in response to the request. The SAO is then forwarded to the consular officer

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00320 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.127

adjudicating the visa, who has the authority to issue or deny visa applications. Individuals that are watchlisted at the time of their visa application could be identified through this process.

The second State Department process supported by the TSC is the Visa Revocation Program. The Visa Revocation Program was initiated after 9/11 and is designed to identify individuals who may have received visas prior to that person being identified as a known or suspected terrorist. Every day, the Department of State automatically generates a report that identifies all individuals with a valid visa that could potentially match a person in the TSDB. State officers compare information in CLASS (exported from TSDB), to existing records of visa holders in the Department of State's Consular Consolidated Database (CCD). This report is then evaluated by the State Department experts at the TSC who determine whether there is a positive match to a watchlisted individual. If there is a positive match, then the TIDE record and related derogatory information is made available to the Department of State for review. The Secretary of State holds broad discretionary authority to revoke a visa. Therefore, TSC forwards the information to the Department of State's Visa Office to determine whether to revoke the visa. Individuals that are watchlisted in TSDB after receiving their visas can be identified through this process.

TECS

TECS serves as the Department of Homeland Security's primary lookout system and receives daily exports of TSDB records from the TSC. Additionally, TECS receives non-terrorist related subject records from more than twenty federal agencies, including a wide spectrum of data, and provides alerts for a variety of law enforcement needs. U.S. Customs and Border Protection (CBP) is the principal owner and primary user of TECS and uses the system to screen individuals at air ports, land, and sea ports of entry. Through TECS, CBP screens against the Terrorist Watchlist at all 327 ports of entry and by all of the 15 pre-clearance offices located in Canada, the Caribbean, and Ireland. They also use the Terrorist Watchlist to conduct screening operations at international mail and cargo facilities. Similar to CLASS, TECS accepts nearly all records from the TSDB. For subjects in TSDB, CBP is alerted to their travel when a commercial airline forwards the passenger manifest to CBP using the Advanced Passenger Information System (APIS). APIS enhances border security by providing officers with pre-arrival and departure manifest data on all passengers and crew members

No Fly and Selectee List

The No Fly and Selectee lists are unique among TSDB subsets in that they are the only subsets within the Terrorist Watchlist that have their own substantive minimum derogatory criteria requirements, which are considerably more stringent than the reasonable suspicion standard required for inclusion in TSDB itself. Following the creation of the TSC in 2003, the Homeland Security Council Deputies Committee established the initial terrorist screening nomination criteria for the No Fly and Selectee lists in October 2004. At that time, the No Fly list consisted of substantive derogatory criteria that focused attention on individuals intending to commit acts of terrorism against civil aviation or the domestic homeland. Over time, that initial criteria proved to be too restrictive. Consequently, in February 2008, the Homeland Security Council Deputies Committee approved additional criteria that served to broaden the scope of

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00321 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.128

terrorists eligible for the No Fly list. In other words, the criteria to place individuals on the No Fly list has broadened to make the No Fly list more inclusive to respond to additional terrorism threats. The Department of Homeland Security Office of Inspector General recognized the significance of the additional criteria when, in a May 2009 report, it stated, "Major security gaps have been addressed by adding No Fly criteria."[1]

For international terrorists, the process to be included on the No Fly list begins, as it does with every nomination, with a federal agency nominating an individual to NCTC for inclusion in TIDE. NCTC analysts review the nomination to ensure it meets nomination criteria and then forward the nomination to the TSC. Analysts at the TSC perform a comprehensive review of the nomination, which includes a review of the derogatory information contained in TIDE and the FBI's Automated Case System. During this process, if there is a reasonable suspicion that the individual is engaging in terrorism or terrorist activity, the terrorist would be added to the TSDB. Placement on the No Fly list requires two components, sufficient biographical information and sufficient derogatory information. If additional information existed to satisfy any of the substantive derogatory criteria and the minimum biographic criteria for the No Fly list, the terrorist's name would be exported to the No Fly list as well. If the analyst reviewing the No Fly nomination determines that there is insufficient information to warrant inclusion on the No Fly list, the nomination is forwarded to the TSA (Office of Intelligence and/or the Federal Air Marshal Service (FAMS)) subject matter experts at the TSC for further analysis and a final recommendation. The TSA subject matter expert will review the nomination and all accessible derogatory information associated with the individual and apply the No Fly and Selectee list criteria to that information. Based upon that review and analysis, the TSA/FAMS subject matter expert will then decide based upon that criteria whether the individual will be included on either the No Fly or Selectee list.

Inclusion on the No Fly list prohibits a potential terrorist from boarding a commercial aircraft that departs or arrives in the United States. It also prohibits an airplane carrying an individual on the No Fly list from transiting United States airspace. The Selectee list is used to provide the individual with a secondary screening. Currently, TSA provides the No Fly and Selectee list to commercial air carriers who are then responsible for passenger prescreening against the No Fly and Selectee lists. With the implementation of the Department of Homeland Security's Secure Flight Program, the U.S. Government will assume the responsibility of passenger prescreening against the No Fly and Selectee lists, which will improve the overall effectiveness of this process.

Actions Since December 25, 2009

Before December 25, 2009, TSC did not receive a nomination to watchlist Umar Farouk Abdulmutallab and, as a result, he was not watchlisted in TSDB. Following the attempted terrorist attack, the President of the United States initiated a review of the facts that permitted Umar Farouk Abdulmutallab to board Northwest Airlines Flight 253. In his January 7, 2010 memorandum, the President concluded that immediate actions must be taken to enhance the security of the American people. These corrective actions were also required to ensure that the

[1] US Department of Homeland Security Office of Inspector General, *Role of the No Fly and Selectee Lists in Securing Commercial Aviation,* OIG-09-64, May 2009.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00322 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.129

standards, practices, and business processes that have been in place since the aftermath of 9/11 are appropriately robust to address the evolving terrorist threat facing our Nation in the coming years. As a result, the TSC was given two instructions. The first was to conduct a thorough review of the TSDB and ascertain the current visa status of all known and suspected terrorists, beginning with the No Fly list. That process has now been completed. The second was to develop recommendations on whether adjustments are needed to the watchlisting Nominations Guidance, including biographic and derogatory criteria for inclusion in TIDE and TSDB, as well as the No Fly and Selectee lists. To do so, TSC convened its Policy Board Working Group with representation from NCTC, DHS, CIA, NSA, DOD, DOJ, DOS, and NSC to achieve interagency consensus. That process is underway and TSC is working with its interagency partners to develop appropriate recommendations for consideration by the President.

As of yet, however, there have been no formal changes to watchlisting criteria, including the criteria for inclusion on the No Fly list, since February 2008 when those criteria were last expanded. At the direction of the White House and in conjunction with NCTC, the TSC has made some temporary and limited additions to the watchlist to counter the specific terrorist threat observed on December 25, 2009. As a result, a threat-related target group was identified and individuals from specific high-threat countries already residing in TIDE or TSDB were added to the No Fly and Selectee lists, or upgraded to TSDB if necessary, to prevent future attacks.

Conclusion

As the investigation into the events that allowed Umar Farouk Abdulmutallab to board Flight 253 continues, the TSC remains focused on fulfilling its Presidential and interagency mandates to share terrorist screening information with our domestic and foreign partners. We have a standing commitment to improve our operational processes, to enhance our human capital and technological capabilities, and to continue to protect Americans from terrorist threats while protecting privacy and safeguarding their civil liberties. Terrorist Watchlisting has been a vital tool in the counterterrorism efforts of the United States Government and will continue to be so in the future. Chairman Lieberman, Ranking Member Collins and members of the Committee, thank you for the opportunity to address this Committee. I look forward to answering your questions.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00323 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.130

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

TRANSPORTATION SECURITY ADMINISTRATION

Statement of

GALE D. ROSSIDES

ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Before the

COMMITTEE ON HOMELAND SECURITY & GOVERNMENT AFFAIRS

UNITED STATES SENATE

March 10, 2010

Good morning Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. Thank you for the opportunity to appear today to discuss the steps the Transportation Security Administration (TSA) has taken in response to the attempted terrorist attack on Northwest Flight 253. I appreciate the Committee's leadership in the aftermath of the attack, and your steadfast efforts to ensure the security of the American people.

The attempted attack on Northwest Flight 253 on December 25 was a powerful reminder that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. As Secretary of Homeland Security Janet Napolitano has testified at recent hearings, this Administration is determined to thwart terrorist plots and disrupt, dismantle, and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just TSA, but components

56838.131

across the Department of Homeland Security and many other federal agencies as well as state, local, tribal, territorial, private sector and international partners.

Today I want to describe the role that TSA currently performs in aviation security, how TSA responded in the immediate aftermath of the attempted Christmas Day attack, and how we are moving forward to further bolster aviation security.

TSA's Role in Multiple Layers of Defense

Since 9/11, the U.S. government has employed multiple layers of defense across several departments and agencies to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

Passenger Identity Verification

As one critical layer of defense, DHS conducts pre-departure passenger identity verification in partnership with the airline industry and foreign governments in order to prevent known or suspected terrorists from boarding a plane bound for the United States or, as appropriate, to identify them for additional screening. DHS uses the Terrorist Screening Database (TSDB), managed by the FBI's Terrorist Screening Center, to determine who may board, who requires further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

Specifically, to help make these determinations, DHS uses the No-Fly List and the Selectee List, two important subsets within the TSDB. Individuals on the No-Fly List should not receive a boarding pass for a flight to, from, over, or within the United States. Individuals on the

56838.132

Selectee List must go through additional security measures, including a full-body pat-down and a full physical examination of personal effects.

Through TSA's Secure Flight Program, the Department is making an important change to the process of matching passenger identities against the No-Fly List and Selectee List, and fulfilling an important recommendation of the 9/11 Commission. Previously, responsibility for checking passenger manifests against these lists rested with the air carriers themselves. Under the Secure Flight program, DHS began to transfer this responsibility to TSA in 2009, and the transition is targeted for completion by the end of this year. In addition to creating a more consistent matching process for all domestic and international travel to the United States and strengthening the effectiveness of redress in preventing misidentifications, Secure Flight will flag potential watchlist matches and immediately trigger law enforcement notification and coordination.

Screening Passengers and Baggage

Another layer of defense in which TSA plays a critical role is the screening of passengers and their baggage. TSA screens passengers and baggage at airports in the United States, but not in other countries. Physical screening at foreign airports is conducted by the foreign government, air carriers, or by the respective airport authority.

Domestically, TSA employs a layered approach to security, which includes measures both seen and unseen by travelers. The 48,000 Transportation Security Officers at hundreds of airports across the United States screen 1.8 million passengers and their baggage every day using advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines, vapor trace machines that detect liquid explosives, Advanced

56838.133

Imaging Technology, full-body pat-downs, explosives detection systems, Bomb Appraisal Officers, and Behavior Detection Officers – both at the checkpoint and throughout the airport. Through programs such as the Aviation Direct Access Screening Program, TSA also uses random and unpredictable measures to enhance security throughout the airport perimeter and in limited access areas of airports. The $1 billion in Recovery Act funds provided to TSA for checkpoint and checked baggage screening technology have enabled TSA to greatly accelerate deployment of these critical tools to keep passengers safe.

In-Flight Security

To support in-flight security, Federal Air Marshals (FAM) are deployed on high-risk domestic and international flights where international partners allow FAMs to enter their country on U.S.-flagged carriers. Thousands more volunteer pilots serve as armed, deputized Federal Flight Deck Officers on domestic flights. Additionally, armed law enforcement officers from federal, state, local, and tribal law enforcement agencies that have a need to fly armed provide a force multiplier on many flights.

International Screening Standards

Because TSA does not conduct screening at international airports, TSA works closely with our foreign partners to ensure international screening standards are followed- particularly for flights bound to the U.S. TSA annually conducts approximately 300 airport assessments at foreign airports using International Civil Aviation Organization (ICAO) standards and inspections of foreign and U.S. air carriers that fly to the United States using TSA standards. If an airport does not meet these standards, TSA works with the host government to rectify the

56838.134

deficiencies and raise airport security to an acceptable level. Ultimately, it is the foreign government that must work to address these security issues. If non-compliance with international standards continues long-term, TSA may recommend suspension of flight service from these airports to the United States.

In addition, TSA inspects all U.S. and foreign air carriers that fly to the United States from each airport that is a last point of departure to ensure compliance with TSA standards and directives. Should air carrier security deficiencies exist, TSA works with the air carrier to raise compliance to an acceptable level.

Response to the Christmas Day Attack

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. TSA directed the Federal Aviation Administration to apprise 128 U.S.-bound international flights from Europe of the attempted attack and to ask them to maintain heightened vigilance on their flights. Increased security measures were put in place at domestic airports, including additional explosive detection canine teams, state and local law enforcement, expanded presence of Behavior Detection Officers, and enhanced screening. TSA conducted calls with all major airlines and the Air Transport Association, and issued Security Directives and Emergency Amendments for all international flights to the U.S., which mandated enhanced screening prior to departure and additional security measures during flight.

In addition to TSA's outreach, DHS was in close contact with Congress, our international partners, and state and local officials across the country. DHS and the FBI issued a joint bulletin on the attempted attack to state and local law enforcement throughout the nation and distributed

56838.135

it to all Homeland Security Advisors, regional fusion center directors and Major City Homeland Security Points of Contact in the country.

On January 3, DHS/TSA issued a new Security Directive, effective on January 4 and still operational today, which includes security measures developed in consultation with law enforcement officials and our domestic and international partners. This Security Directive mandates that every individual flying into the U.S. from anywhere in the world traveling from or through nations that are state sponsors of terrorism[1] or other countries of interest will be required to go through enhanced screening. The directive also increases the use of enhanced screening technologies and mandates threat-based and random additional screening for passengers on U.S. bound international flights. These measures are being implemented with extraordinary cooperation from our global aviation partners

Steps Forward to Improve Aviation Security

While these immediate steps helped strengthen our security posture to face current threats to our country, as President Obama has made clear, we need to take additional actions to address the systemic vulnerabilities highlighted by this failed attack. At President Obama and Secretary Napolitano's direction, DHS and TSA are pursuing five key objectives to enhance the protection of air travel from acts of terrorism.

Watchlists

First, DHS is working with our interagency partners to re-evaluate and modify the criteria and process used to build the TSDB, including adjusting the process by which names are added

[1] The State Department currently lists Cuba, Iran, Sudan, and Syria as state sponsors of terrorism.

56838.136

to the No-Fly and Selectee Lists. The Department's ability to prevent terrorists from boarding flights to the United States depends upon these lists and the criteria used to create them. As an entity that is primarily a consumer of this intelligence and the operator of programs that rely on these lists, DHS is working closely with our partners in the Intelligence Community to make clear the kind of information DHS needs from the watchlist system.

DHS/ DOE Partnership

Second, DHS has established a new partnership with the Department of Energy (DOE) and its National Laboratories in order to use their expertise to bolster security. The Deputy Secretaries of Homeland Security and Energy are leading the effort to bring the paramount capabilities and critical resources of the DOE National Laboratories to bear on developing advance technical solutions to key aviation security challenges. This partnership will focus on advancing current technology, assessing system capabilities to determine gaps, and developing emerging technologies to fill those gaps in an efficient and effective manner.

Two years ago, DHS and DOE formed the National Explosive Engineering Sciences Security (NEXESS) Center, a consortium of National Laboratories including Sandia National Laboratory, Los Alamos National Laboratory, and Lawrence Livermore National Laboratory, to provide an agile and aggressive means to anticipate and understand explosive threats and to develop countermeasures to protect the homeland. The NEXESS Center provides informed scientific analysis for short- to mid-term priority assessments as well as mid- to long-term research and technology development. The Deputy Secretaries of both DHS and DOE are working collaboratively to strengthen these efforts in light of the December 25 attempted attack.

56838.137

TSA is also working closely with the DHS Transportation Security Laboratory (TSL) in technology development. The TSL, operated by DHS Science & Technology, performs extensive qualification testing for all of TSA's explosives screening equipment.

Enhanced Screening Technology

Third, TSA is aggressively pursuing the deployment of enhanced screening technology to domestic airports and encouraging our international partners to do the same. While no technology is a silver bullet in stopping a terrorist attack, a number of technologies, when employed as part of a multi-layered security strategy, can increase our ability to detect dangerous materials.

To this end, TSA will accelerate deployment of Advanced Imaging Technology to increase capabilities to identify materials such as those used in the attempted December 25 attack. These efforts are already well underway. TSA currently has 40 machines deployed at nineteen airports throughout the United States and purchased 150 additional AIT units last September under the American Recovery and Reinvestment Act of 2009. This year, TSA expects to deploy at least 450 additional units across the country. The Administration's Fiscal Year 2011 budget calls for purchasing and installing an additional 500 AIT units, which would bring the total number of AIT units to approximately 1,000. The detection capabilities of AIT units are one part of a successful technology security initiative, but it is also critical that TSOs have the necessary training to resolve an anomaly identified by the AIT operator. TSA is working to improve both the detection capability of the units and the ability of screening personnel to resolve an anomaly, while being respectful of personal privacy, dignity, and civil rights and

56838.138

liberties. The Administration's Fiscal Year 2011 budget also includes additional personnel to operate these AIT machines.

DHS is also increasing assets in the area of canine teams, explosives detection equipment, and highly trained security personnel to strengthen our abilities to find dangerous materials and stop dangerous people from boarding aircraft. Nearly 950 Advanced Technology X-ray machines have been deployed to U.S. airports to enhance the screening of carry-on bags. Additional machines will follow this year and include automated detection software to improve their capability. TSA has expanded the random use of Explosive Trace Detection (ETD) machines, which can be effective against a wide scope of explosives, to screen both passengers and bags. The Administration's Fiscal Year 2011 budget request calls for $60 million to purchase approximately 800 portable ETD machines. The FY 2011 budget also requests funding for a substantial increase of explosives detection canines by adding an additional 275 teams. Further, the budget seeks funding for an additional 350 Behavior Detection Officers.

Aviation Law Enforcement

Fourth, DHS will strengthen the presence and capacity of aviation law enforcement. Beginning this month, as an interim measure, we have deployed additional law enforcement officers from across DHS- including the Secret Service, Customs and Border Protection, Immigration and Customs Enforcement, and the U.S. Coast Guard- to assist Federal Air Marshals. In January, these highly trained officers participated in an accelerated specialized training program led by the FAMS on the unique methods employed to protect and defend an aircraft. This will allow for an immediate further increase in FAMS coverage of international

56838.139

flights. The President's FY 2011 budget request also increases funding to sustain long-term FAMS coverage on domestic and international flights.

International Partnerships

Fifth, as mentioned earlier, DHS will continue to work with international partners to strengthen international security measures and standards for aviation security. Much of our success in ensuring that terrorists do not board flights to the United States is dependent on what happens in foreign airports and the commitment of our foreign partners to enhance security.

Last month, DHS leadership embarked upon an aggressive international outreach initiative to enhance international aviation security standards and practices- particularly for international flights bound for the United States. In early January, Deputy Secretary Lute and other senior Department officials traveled to Africa, Asia, Europe, the Middle East, Australia, and South America to meet with international leadership on aviation security. In these meetings, they reviewed security procedures and technology being used to screen passengers on U.S.-bound flights and worked on ways to bolster our collective tactics for defeating terrorists.

Later in January, Secretary Napolitano traveled to Toledo, Spain and Geneva, Switzerland to meet with her international counterparts and the private sector air carriers on aviation security. In Spain, at the invitation of the Spanish Minister of Interior, the Secretary participated in the first organizational meeting of the Spanish EU Presidency of Justice and Home Affairs ministers, a plenary of thirty-three countries. At this meeting, there was broad consensus and a clear sense of urgency to take immediate action to strengthen security measures, as the Secretary and her European counterparts signed a joint declaration affirming their collective commitment to strengthening information sharing and passenger vetting, deploying

56838.140

additional proven security technologies, and bolstering international aviation security standards. There was similarly strong consensus in Geneva, where the Secretary met with the leaders of the International Air Transport Association, which represents approximately 230 airlines and more than 90 percent of the world's air traffic. They agreed that government and the private sector must work collaboratively both to develop enhanced international security standards and-most importantly-to implement them effectively.

These meetings were the first in a series to bring about international agreement on stronger aviation security standards and procedures. Over the next few months, the International Civil Aviation Organization (ICAO) will facilitate several regional aviation security meetings to build on the progress made in Toledo and Geneva. TSA, specifically, has also developed an aggressive timeline and corresponding strategy for international engagement and outreach through our Office of Global Strategies. Focusing on priority areas designed to affect the greatest change in international civil aviation security, TSA is boosting its work with foreign government counterparts and industry stakeholders to raise awareness of the threat and to encourage specific enhancements in security measures worldwide. These priorities include: developing a common view and understanding of the threat to civil aviation; enhancing international standards for civil aviation security through ICAO; conducting security audits and ensuring robust oversight; encouraging the use of technological and non-technological measures to prevent and deter terrorist activity in the civil aviation sector; developing cooperative agreements for information sharing with key foreign government partners; providing training and related technical assistance to develop and enhance sustainable security practices in partner countries; and working with appropriate foreign government counterparts to enhance their authorities in their national aviation security domain. This targeted coordination and

56838.141

collaboration, through both bilateral and multilateral forums, will continue to advance our key security objectives and improve the overall level of security of international civil aviation while fostering our international partnerships and relations that are critical to this effort.

In all of these action areas to bolster aviation security, we are moving forward with a determination to safeguard the privacy and rights of travelers.

Conclusion

In closing, Mr. Chairman, TSA is taking aggressive action in the wake of the failed Christmas Day bombing. We are expanding and improving the use of technology, strengthening aviation security protocols with our foreign partners, developing long-term law enforcement capacities in aviation security, collaborating across the Administration in developing the next generation of aviation security technology, working to streamline and improve the U.S. watchlist matching process for air travelers, and strengthening a TSA workforce that is highly trained, agile and dedicated to this mission. TSA and DHS are prepared to meet the challenge.

Thank you for your continued assistance to TSA and for the opportunity to discuss these steps with you today. I would be pleased to respond to your questions.

56838.142

TESTIMONY OF

DAVID V. AGUILAR

ACTING DEPUTY COMMISSIONER
U.S. CUSTOMS AND BORDER PROTECTION
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE

SENATE HOMELAND SECURITY AND
GOVERNMENTAL AFFFAIRS COMMITTEE

MARCH 10, 2010

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee. Thank you for the opportunity to appear today to discuss the steps U.S. Customs and Border Protection (CBP) has taken in response to the attempted terrorist attack on Northwest Flight 253. I appreciate the Committee's leadership in the aftermath of the attack, and your steadfast efforts to ensure the security of the American people.

The attempted attack on Northwest Flight 253 on December 25 was a powerful reminder that terrorists will go to great lengths to defeat the security measures that have been put in place since September 11, 2001. As Secretary Napolitano has testified at recent hearings regarding the attempted attack, this Administration is determined to thwart terrorist plots and disrupt, dismantle, and defeat terrorist networks by employing multiple layers of defense that work in concert with one another to secure our country. This is an effort that involves not just CBP, but components across the Department of Homeland Security and many other federal agencies as well as state, local, tribal, territorial, private sector and international partners.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00336 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.143

Today I want to describe the role that CBP currently performs in aviation security and the enhanced security measures implemented in the aftermath of the attempted Christmas Day attack.

CBP's Role in Multiple Layers of Defense

Since 9/11, the U.S. government has employed multiple layers of defense across several departments and agencies to secure the aviation sector and ensure the safety of the traveling public. Different federal agencies bear different responsibilities, while other countries and the private sector – especially the air carriers themselves – also have important roles to play.

CBP is responsible for securing our Nation's borders while facilitating the movement of legitimate travel and trade vital to our economy. Our purview spans more than 5,000 miles of border with Canada and 1,900 miles of border with Mexico. CBP is the largest uniformed, federal law enforcement agency in the country, with over 20,000 Border Patrol Agents operating between the ports of entry and more than 20,000 CBP officers stationed at air, land, and sea ports nationwide. These forces are supplemented with more than 1,100 Air and Marine agents, and 2,300 agricultural specialists and other professionals. In FY 2009 alone, CBP processed more than 360 million pedestrians and passengers, 109 million conveyances, apprehended over 556,000 illegal aliens between our ports of entry, encountered over 224,000 inadmissible aliens at the ports of entry, and seized more than 5.2 million pounds of illegal drugs. Every day, CBP processes over one million travelers seeking to enter the United States by land, air or sea.

In order to counter the threat of terrorism and secure our borders, CBP relies on a balanced mix of professional law enforcement personnel, advanced technologies and

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00337 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.144

fully modernized facilities and infrastructure both at and between the ports of entry. We deploy a cadre of highly trained agents and officers who utilize state of the art technologies to quickly detect, analyze and respond to illegal breaches across the borders. These personnel rely upon a solid backbone of tactical infrastructure to facilitate their access to border areas while impeding illegal entry by persons or vehicles into the United States. CBP Officers utilize advanced targeting, screening and inspection technologies to quickly identify persons or cargo that warrant additional scrutiny without unduly impeding the traveling public or commerce.

CBP and Intelligence

In 2007, CBP created the Office of Intelligence and Operations Coordination (OIOC), which serves as the situational awareness hub for CBP, providing timely, relevant information and actionable intelligence to operators and decision-makers and improving coordination of CBP-wide operations. Through prioritization and mitigation of emerging threats, risks and vulnerabilities, OIOC enables CBP to better function as an intelligence-driven operational organization. The OIOC serves as a single, central repository for agency-wide intelligence, while exploring new ways to analyze and fuse information.

As part of our efforts to screen passengers bound for the United States, CBP is a consumer of the U.S. Government's consolidated terrorist watchlist, which we use to help keep potential terrorists off flights bound for the United States and to identify travelers that require additional screening. Specifically, DHS uses the Terrorist Screening Database (TSDB), managed by the Terrorist Screening Center, as well as other information provided through the Intelligence Community, to determine who may board

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00338 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.145

flights, who requires further screening and investigation, who should not be admitted, or who should be referred to appropriate law enforcement personnel.

National Targeting Center-Passenger (NTC-P)

A key tool for DHS in analyzing, assessing, and making determinations based on the TSDB and other intelligence information, is the National Targeting Center (NTC), run by CBP. The NTC is a 24/7 operation, established to provide tactical targeting information aimed at interdicting terrorists, criminal actors and prohibited items. Crucial to the operation of the NTC is CBP's Automated Targeting System (ATS), a primary platform used by DHS to match travelers and goods against screening information and known patterns of illicit activity. 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).

This year, Immigration and Customs Enforcement (ICE) began deploying Visa Security Program (VSP) personnel to the NTC-P to augment and expand current operations. Through the VSP, ICE stations agents at embassies and consulates to assist the State Department in identifying visa applicants who may present a security threat. The focus of the VSP and NTC-P are complementary: the VSP is focused on identifying terrorists and criminal suspects and preventing them from reaching the United States, while the NTC-P provides tactical targeting and analytical research in support of preventing terrorist and terrorist weapons from entering the United States. The co-location of VSP personnel at the NTC-P has helped increase communication and information sharing.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00339 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.146

Safeguards for Visas and Travel

One of the first layers of defense in securing air travel involves safeguards to prevent dangerous people from obtaining visas, travel authorizations and boarding passes. To apply for entry to the United States prior to boarding flights bound for the U.S. or arriving at a U.S. port of entry, most foreign nationals need visas – issued by a U.S. embassy or consulate – or, if eligible to travel under the Visa Waiver Program (VWP) country, travel authorizations issued through the Electronic System for Travel Authorization (ESTA).[1]

Issuing visas is the responsibility of the Department of State (DOS), which screens all visa applicants biographic data against the TSDB for terrorism-related concerns and screens their biometric data (fingerprints and facial recognition) against other U.S. government databases for security, criminal and immigration violation concerns. For individuals traveling under the VWP, DHS operates ESTA, a web-based system through which individuals must apply for travel authorization prior to traveling to the United States. ESTA enables CBP to conduct enhanced screening of VWP applicants in advance of travel to the United States in order to assess whether they could pose a risk to the United States, including possible links to terrorism. On January 20, 2010, CBP began its transition to enforce ESTA compliance for air carriers, requiring all foreign nationals to present a valid authorization to travel to the United States at the airport of departure.

[1] Exceptions would be citizens of countries under other visa waiver authority such as the Western Hemisphere Travel Initiative or the separate visa waiver program for Guam and the Commonwealth of the Northern Mariana Islands, or those granted individual waivers of the visa requirement under the immigration laws.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00340 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.147

Pre-departure Screening

When a traveler purchases a ticket for travel to the United States, a Passenger Name Record (PNR) may be generated in the airline's reservation system. PNR data contains various elements, which may include optional information on itinerary, co-travelers, changes to the reservation, and payment information. CBP receives PNR data from the airline at various intervals beginning 72 hours prior to departure and concluding at the scheduled departure time. CBP officers utilize the Automated Targeting System – Passenger (ATS-P) to evaluate the PNR data against "targeting rules" that are based on law enforcement data, intelligence and past case experience.

On the day of departure, when an individual checks-in for their intended flight, the basic biographic information from the individual's passport is collected by the air carrier and submitted to CBP's Advance Passenger Information System (APIS). APIS data, which carriers are required to provide to DHS at least 30 minutes before a flight for all passengers and crew on-board, contains important identifying information that may not be included in PNR data, including verified identity and travel document information such as a traveler's date of birth, citizenship, and travel document number. Carriers are required to verify the APIS information against the travel document prior to transmitting it to CBP. DHS screens APIS information on international flights to or from the United States against the TSDB, as well as against criminal history information, records of lost or stolen passports, and prior immigration or customs violations and visa refusals. APIS is also connected to Interpol's lost and stolen passport database for routine queries on all inbound international travelers.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00341 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.148

Another layer in the screening process is the Immigration Advisory Program (IAP), which stations CBP officers at nine airports in seven countries in coordination with the host foreign governments. CBP's National Targeting Center provides the IAP officers with non-U.S. Citizen and non-Legal Permanent Resident matches to the TSDB, of which the No Fly list is a subset. CBP also flags anyone whose U.S. visa has been revoked, whose Electronic System for Travel Authorization (ESTA) has been denied, who is using a foreign lost or stolen passport, or who is included on a Public Health Record provided by the Centers for Disease Control and Prevention.IAP officers can make "no board" recommendations to carriers and host governments regarding passengers bound for the United States who may constitute security risks, but do not have the authority to arrest, detain, or prevent passengers from boarding planes.

Screening while en-route to the United States and upon arrival

While flights are en route to the United States, CBP continues to evaluate the APIS and PNR information submitted by the airlines. At this point, a further assessment of an individual's admissibility into the United States is conducted, and a determination is made as to whether an individual requires additional screening prior to admission.

Upon arrival in the United States, travelers present themselves to a CBP officer for inspection. Based on the information garnered during the in-flight analysis, as well as the CBP officer's observations at the port of entry, a determination is made as to whether the traveler should be referred for a secondary inspection or admitted to the United States.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00342 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.149

Enhanced Security Measures Implemented Since the Christmas Day Attack

Following the first reports of an attempted terrorist attack on Northwest Flight 253 on December 25, DHS immediately put in place additional security measures. Since then, CBP has undertaken a number of initiatives to enhance our security posture.

IAP Referrals

As explained above, CBP officers stationed abroad under the IAP receive referrals from the NTC-P based on matches against the TSDB. Following the attempted attack in December, the NTC-P, in coordination with the OIOC, has expanded the information referred to IAP's to include all aliens that the State Department has identified as actually, or likely, having engaged in terrorist activity as well, as existed in that case.. NTC-P and OIOC continue to work with the Intelligence Community to develop new rules to address the ever-changing threat, while implementing specific operations to address these threats.

Referrals for non-IAP Airports

On January 10, 2010, CBP also began pre-screening passengers traveling from non-IAP locations through the ATS-P framework. To accomplish this goal, the NTC-P works in coordination with officers assigned to the Regional Carrier Liaison Groups (RCLG). The RCLG are established in Honolulu, Miami and New York and provide regional points of contact and coordination between international carriers, foreign immigration authorities and other DHS entities. The RCLG respond to carrier inquiries concerning the validity of travel documents presented or admissibility of travelers. Additionally, CBP officers at the NTC-P work with the RCLG officers to make recommendations to foreign carriers that boarding be denied (off-loads) to individuals traveling to the United States who have been identified as being national security related

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00343 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.150

threats, ineligible for admission or who are traveling on fraudulent or fraudulently obtained documents prior to boarding a flight to the United States. However, the final decision to board or not board remains with the carrier. This pre-departure initiative mirrors our IAP efforts for flights originating from airports that do not currently have an IAP presence.

Enhanced Operational Protocols

At home and abroad, CBP officers have been briefed on the current threat stream and continue to work with our international partners, air carriers, local police, border control and counterterrorism authorities to recommend passengers traveling to and entering the U.S. for additional screening as needed. CBP has implemented enhanced operational protocols at 15 preclearance locations and all 300 plus ports of entry in the United States. At airports, CBP has enhanced reviews of all incoming advanced passenger manifests based on current threats and have increased pre and post-primary operations. At U.S. ports of entry, Passenger Analysis Units (PAU), and Counter Terrorism Response (CTR) teams continue carrying out targeted enforcement inspections, and have increased reviews of cargo manifest systems/databases by our Advance Targeting Unit (ATU) teams, and vehicle trunk inspections and truck cab checks. At POEs, the CTR team will normally be formed from CBP Officers assigned to special teams, or who possess prior counter-terrorism, antiterrorism, or intelligence-related training or experience. These officers are then provided additional training in order to target persons or cargo that may warrant additional scrutiny. PAU and ATU are specifically designed to target passengers or cargo that may require CTR examination before they arrive at the POE. At seaports, CBP has heightened screening with Non

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00344 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.151

Intrusive Inspection (NII) equipment of all cargo from countries of interest, and increased cargo and port perimeter sweeps.

Through intelligence sharing agreements, CBP continues to work with our counterparts in the United Kingdom, Canada, and Mexico, as well as CBP Attachés and representatives around the world, to share information as necessary and appropriate.

Conclusion

The attempted attack on Christmas Day serves as a stark reminder that terrorists motivated by violent extremist beliefs are determined to attack the United States. President Obama and Secretary Napolitano have made clear that we will be unrelenting in using every element of our national power in our efforts around the world to disrupt, dismantle, and defeat al-Qaeda and other violent extremists.

While we address the circumstances behind this specific incident, we must also recognize the evolving threats posed by terrorists, and take action to ensure that our defenses continue to evolve in order to defeat them. We live in a world of ever-changing risks, and we must move as aggressively as possible both to find and fix security flaws and anticipate future vulnerabilities. CBP will continue to work with our colleagues in DHS and the Intelligence Community to address this ever-changing threat.

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for this opportunity to testify. I look forward to answering your questions.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00345 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.152

Post-Hearing Questions for the Record
Submitted to Russell E. Travers
From Senator Joseph I. Lieberman

"The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening"
March 10, 2010

1. NCTC Director Michael Leiter testified before this Committee on January 20th that NCTC does not have the capability to conduct a single search across intelligence community databases but instead must query each database individually. An internal assessment of the terrorist watch list process undertaken by the DNI last year supports Director Leiter's statement and highlights the ways in which the stovepiped information architecture within the intelligence community makes it challenging for NCTC analysts to search relevant databases and validate watchlisting nominations. In assessing the watchlisting process, this internal report points out that NCTC analysts lack the ability to conduct a Google-like search across databases. Instead, they need to separately log-on to different networks and data sources. This obviously results in an inefficient use of time—and as we know, time is all too often short. The assessment also notes that NCTC analysts often have "limited source information" and "don't know what they don't know."

    a. What is being done to enhance the efficiency of the analytic processes that support watchlisting, and to ensure that analysts are able to discover all the information that exists across the government's intelligence databases about a person who has been nominated – or build the case for NCTC-generated nominations?
    b. Are there specific types of information that NCTC analysts are unable to access when they are reviewing watchlisting nominations - for example, certain types of compartmented information? Without going into details, what steps are being taken in the wake of the Christmas Day attack to remove such barriers and ensure that such information can be queried where appropriate?

2. What is being done in the wake of the Christmas Day attack to develop capabilities that would allow NCTC to improve automated discovery of potential threat-related information in a way that would support the watchlisting system? What exactly are the legal or policy obstacles that need to be overcome in order to implement such automated capabilities?

Responses to the above Questions for the Record were submitted as "for official use only" and are on file with the Committee.

56838.378

Post-Hearing Questions for the Record
Submitted to Gale D. Rossides and David V. Aguilar
From Senator Joseph I. Lieberman

Question#: 1

Topic: Global API

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: Our ability to pre-screen international travelers against our watchlists and other databases is a crucial component of our national security. The President's budget submission would eliminate funding for the Global Advance Passenger Information program (Global API). Global API seeks to address a weakness in our prescreening system by reaching agreements with other countries to provide us with information about passengers on flights that do not have a nexus to the United States that is, flights that are not coming to the U.S. This is important because if someone purchases their ticket to the United States in two separate transactions, spending perhaps a day or two in another country in between their two flights, we currently have no way to know about their travel until they show up at the airport for their U.S.-bound flight. The Christmas day attack has shown us that this prescreening needs to begin as soon as possible and Global API is an important piece of the puzzle.

Why is DHS seeking to eliminate funding for the Global API program? How will DHS ensure that alternative funding is available should other countries seek to participate in the program during FY2011, given that the Department is also proposing a cut in the CBP travel budget?

Response: While the FY 2011 budget request does not sustain the $3M FY 2010 initiative for the Global API program, CBP is not eliminating its commitment to the program. CBP is continuing outreach to the countries with significant interest in the program. Should an opportunity with an interested country present itself, CBP would identify internal funding and make the appropriate notifications, to support such a request. Additionally, CBP would request the funding in future budget requests.

Question: Would DHS support Congressional action to expand the current passenger prescreening programs for international flights to ensure that CBP and other agencies have access to the identifying biographical information required to check all of our government's intelligence and crime databases at least 24 hours before an airplane departs for the United States?

Response: Commercial air carriers must transmit Advance Passenger Information System (APIS) data no later than 30 minutes prior to securing the aircraft doors for a batch transmission of passenger data or up to the time of securing the aircraft doors for interactive Automated Quick Query (AQQ) submissions of individual passenger data. CBP also requires commercial air carriers to provide access to available Passenger Name

56838.153

Question#: 1

Topic: Global API

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Record (PNR) data starting at 72 hours before departure. Many passenger name records contain incomplete information, which limits CBP's ability to conduct terrorist watchlist screening, however; this will change with the full implementation of the Transportation Security Administration's (TSA) Secure Flight program.

Under Secure Flight, carriers will be required to collect and provide passenger information including Full Name, Date of Birth and Gender to TSA 72 hours prior to departure for purposes of security screening. When Secure Flight is fully deployed for international air carriers (by December 31, 2010), CBP will receive this passenger information through the PNR data requirement resulting in enhanced screening capabilities for CBP.

Requiring additional passenger information and additional time for screening, beyond current APIS and PNR requirements, would necessitate changes to existing processes. Requiring travelers to formalize plans to travel to or from the United States at least 24 hours before departure would also preclude all last-minute travel.

56838.154

Question#: 2

Topic: TSDB

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: Over 400,000 individuals have been identified as known or suspected terrorists on our Consolidated Terrorist Screening Database (TSDB). Only a small subset of these people, about 12,000, face enhanced physical screening measures at our airports. In the wake of the December 25th attack by Abdulmutallab, we may need to consider whether aviation passengers should be pre-screened against the TSDB, and not just the no-fly or selectee list, to determine if they should be subjected to enhanced physical screening measures. The implications for this type of change may be substantial, and may be different for domestic and international flights. But I believe that the risk of allowing someone who is on our government's list of known or suspected terrorists to board a plane without being subjected to a secondary physical screening is intolerable. If such a person ends up carrying out an attack, the public's confidence in our screening systems would be severely compromised, and rightfully so.

a. What are the current obstacles to subjecting all individuals on the TSDB to a secondary physical screening at the airport? Are our passenger pre-screening systems capable of handling this expansion?

Response: The Department of Homeland Security believes the No Fly and Selectee subsets of the Terrorist Screening Database (TSDB) are appropriate for pre-screening passengers against the watch list. However, as part of DHS efforts to enhance aviation security, as directed by the President in his January 7, 2010 memorandum, DHS has undertaken a comprehensive review to evaluate expanding the scope of subjects watchlisted in the Terrorist Screening Database (TSDB, the U.S. Government's consolidated terrorist watchlist) who should undergo enhanced physical screening prior to boarding an aircraft.

Question:

b. What is DHS's best estimate of how many additional secondary exams would be generated by such an expansion? Are the TSA checkpoints capable of handling additional secondary exams?

Response: The Transportation Security Administration is unable to predict with any accuracy the increase in additional secondary examinations generated by proposed expansions to the Selectee list or use of the fuller TSDB for watchlist matching.

56838.155

Question#: 2

Topic: TSDB

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question:

c. Do these obstacles apply to both international and domestic flights? Would it be feasible to expand the use of the watchlist for secondary screening to international flights bound for the U.S. before doing it for all domestic flights? Have we discussed such a measure with our foreign partners, who would have to carry out the physical screening? Are our international agreements robust enough to ensure that our foreign partners will agree to screen additional people if we expand the selectee list?

Response: Watchlist screening is generally conducted in the same manner for both domestic and international flights. As threat and risk warrant, however, the Transportation Security Administration (TSA) continues to explore mechanisms for enhanced screening for international flights that is informed by real-time threat information and intelligence. Simultaneously, TSA is laying the groundwork for such initiatives with our international partners, and accordingly, TSA continues to meet with foreign partners to discuss a way forward on mitigating the shared threat to international civil aviation security. In order to provide service to the United States, governments must comply with international security standards established by the International Civil Aviation Organization (ICAO), which is the United Nations' specialized agency for aviation matters. These international standards include provisions for the physical screening of passengers and their property. Additionally, air carriers must comply with specific TSA requirements for all flights to the United States. As threat information warrants, these requirements may include the enhanced screening of passengers and their property for U.S.-bound flights, which often is carried out by the relevant host government authorities. Effectively, in many cases, any additional security measures TSA might implement for international inbound flights to the United States beyond the international standards set by ICAO, will be implemented by, and the costs for doing so will be borne by, the relevant foreign government as well as the air carriers. When TSA requirements change, foreign government counterparts and industry stakeholders are notified and given a period of time for implementation. Although challenges frequently arise when changes to these requirements are made, TSA works with its foreign government counterparts to address concerns while at the same time ensuring security requirements are met.

56838.156

Question#: 3

Topic: ESTA

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: The easiest way to get the identifying information that we need about passengers would be to expand the PNR system. However, we continually hear from the airlines that requiring identifying fields to be included in the PNR system would be difficult and expensive for them to implement. There is another option that may be easier to implement. This Committee implemented the Electronic System for Travel Authorization (ESTA) to collect the important identifying information needed by our agencies to match the records of travelers from visa waiver countries. We have been told that the airlines are very close to being able to automatically check for an ESTA as passengers check into their flights and deny boarding if they do not have one. If we expand this system to include all travel to the United States we would know, in advance, the identities of all individuals planning to come to the United States. Because the ESTA system checks all of its enrolled travelers against all of our law enforcement and intelligence databases each day, if someone was granted a visa but subsequently committed a crime or was watchlisted, their ESTA would automatically be invalidated and they would not be allowed to board an airplane.

Does CBP believe that an expansion of the ESTA requirement to include all countries would be useful? What does DHS believe would be the obstacles to expanding the ESTA system to include all travelers to the United States?

The ESTA system currently allows individuals to register only once every two years. It seems to me that one way to know when people are planning to travel to the United States could be to require that they register for an ESTA each time they want to come here. What obstacles would there be to expanding ESTA so that travelers, especially those from non-visa waiver nations, had to register for ESTA each time they booked a flight for the U.S.?

Response: First of all, it should be noted that although ESTA applications generally are valid for two years, CBP performs regular screening of all travelers each and every time they travel to the United States.

The ESTA requirement applies specifically to travelers seeking to travel under the Visa Waiver Program (VWP), as required by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. 110-53). There is currently no legal authority for requiring non-VWP travelers to apply for an ESTA; such travelers instead are required to apply for a visa through the Department of State.

Additionally, carriers are also in process of transitioning to the Transportation Security Administration (TSA) Secure Flight program where carriers are required to provide data to DHS starting 72 hours prior to departure. Under Secure Flight, carriers will be required to provide passenger information including Full Name, Date of Birth and Gender to TSA for security screening.

56838.157

Question#: 4

Topic: visa revocations

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: Almost nine years after 9/11, we do not have an automated way to check passengers against our visa revocation lists. PNR data is currently checked against revocations, but this data is sometimes not robust enough to allow a match to be made. This is a clear weakness in our passenger pre-screening system. We simply cannot afford to allow travelers who have their visas revoked to board airplanes. It is the Committee's understanding that the State Department has been working with DHS to implement an automated system.

What is the current timeline for deploying an automated system for checking visa revocations at the same time the no-fly list is checked?

Response: CBP currently screens travelers destined for the United States for visa revocations via an automated interface with the Department of State systems.

The Intelligence Reform and Terrorism Act of 2004 (IRTPA) (Pub. L. 108-458), enacted December 17, 2004, requires the Federal Government to conduct a terror watchlist screening before a passenger travels on a flight where practicable. On August 23, 2007, the Advance Passenger Information System (APIS) Pre-Departure Final Rule was published in the Federal Register, requiring APIS data pre-departure to enable the CBP system to conduct screening against the no-fly and selectee watch lists and to provide air carriers with the results prior to passengers gaining access to the aircraft.

56838.158

Question#: 5

Topic: Secure Flight

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: Under Secure Flight, all airlines will transmit passenger data for both international and domestic flights to the Secure Flight program. This data will include information such as name and date of birth, which will be used to check the passenger manifest against the appropriate watchlists. It may also include information CBP needs to begin some of the immigration and border security checks it does.

How will DHS manage the various checks component agencies need to perform using information collected under the Secure Flight program, while ensuring that there is sufficient information collected, and that neither agency's process will be impeded or slowed under the umbrella of the Secure Flight program?

What is DHS doing to ensure that this process is not cumbersome for the airlines, and that response times won't be affected by the necessary interagency coordination?

What is the current timeline for full implementation of Secure Flight to all air travel with a United States nexus?

Response: DHS has implemented a layered approach to screening advance passenger information to ensure the timely, thorough, and appropriate level of information-based screening specific to CBP and TSA's respective missions.

CBP has access to available Passenger Name Record (PNR) data for international flights with a nexus to the U.S. beginning at 72 hours prior to departure. CBP screens PNR data against various law enforcement and immigration databases including Terrorist Screening Database (TSDB) records. Additionally, carriers are required to transmit their complete and final passenger manifests through the Advance Passenger Information System (APIS) to CBP no less than 30 minutes prior to securing the aircraft doors (for batch data transmission) or up to the time of securing the aircraft doors (for carriers utilizing the interactive APIS Quick Query (AQQ) transmission process). APIS data includes passenger information that is found on the biographic page of passports, such as full name, date of birth, gender, document number, and country of document issuance.

TSA is implementing the Secure Flight program that requires carriers to provide Secure Flight Passenger Data (full name, date of birth, and gender) beginning at 72 hours prior to the departure of a flight (domestic or international). The Secure Flight program normally screens against the No Fly and Selectee subsets of the TSDB and the Centers for Disease

56838.159

Question#: 5

Topic: Secure Flight

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Control's (CDC) Do Not Board list. As stated in the Secure Flight final rule, TSA may use the full TSDB for Secure Flight screening when warranted based on a specific security threat or other security factors. For example, TSA may receive actionable intelligence that identifies a heightened security risk associated with flights between two cities. TSA may determine that the intelligence, together with the information in the TSDB records, supports using the full TSDB to conduct watchlist matching of passengers on flights between these two cities for the duration of the heightened risk.

TSA anticipates that Secure Flight deployments for U.S. aircraft operators will be completed in spring 2010. TSA has also initiated Secure Flight deployments for foreign air carriers and expects to transition watchlist (No Fly, Selectee, and CDC Do Not Board) matching to Secure Flight for all covered flights, international and domestic, by the end of calendar year 2010.

Once international carriers have transitioned to Secure Flight, carriers will be required to collect and provide passenger information including Full Name, Date of Birth and Gender. CBP will also receive this passenger information through the PNR data requirement resulting in enhanced screening capabilities for CBP beginning at 72 hours prior to departure. CBP will continue to screen PNR and APIS data as part of their border security and immigration admissibility determinations.

DHS has worked closely with the airline industry to provide one information technology conduit through which carriers may provide passenger information and receive timely pre-boarding results that will not impede carrier operations. DHS continues to work closely with interagency stakeholders and the airlines to ensure that program requirements are aligned and resources are managed effectively.

56838.160

Question#: 6

Topic: ICAO

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: The attempted terrorist attack on a Northwest Airlines flight in Detroit last Christmas Day is a sobering reminder of the importance of international cooperation in the fight against terrorism and the need for universally adopted aviation security measures. Since 9/11, the U.S. government has worked closely with the International Civil Aviation Organization (ICAO) to foster international cooperation in aviation security. The ICAO took on the enduring challenge of harmonizing the implementation of aviation security measures worldwide, recognizing that deficiencies in any part of the air transport system constitute a threat to the international community as a whole. Taiwan is a key air transport hub in the Asia Pacific region serving more than 1 million flights and over 40 million passengers each year. Despite this important regional role in the global air transport system, Taiwan has been excluded from ICAO since 1971. Taiwan's lack of participation in the ICAO may contribute to gaps in international aviation security.

What is DHS's assessment of Taiwan's aviation security posture?

Response: At the time of the last TSA Airport Assessment in Taipei, the airport was found to be in compliance with ICAO Annex 17, Standards and Recommended Practices.

Question: Do you believe that allowing Taiwan to join ICAO would be beneficial for international aviation security?

Response: DHS follows the Department of State policy that the United States supports Taiwan's membership in international organizations where statehood is not a prerequisite and supports meaningful participation by Taiwan in organizations where statehood is required. Taiwan's ability to gain official status in ICAO or other United Nations organizations is affected by the fact that Taiwan is not a Member State of the United Nations and does not have observer status at the United Nations General Assembly.

It is U.S. policy to support Taiwan's involvement in international organizations, processes, agreements, and gatherings wherever possible. Our overall goal is to ensure that Taiwan has access to information on international standards, restrictions, quotas, etc., so that it can comply with international regulations and guidelines and benefit from international assistance and advice.

56838.161

Question#: 6

Topic: ICAO

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

We are aware that Taiwan wishes to expand its meaningful participation in ICAO. Given the volume of flights through Taiwan's airspace, there are important practical reasons to support the island's inclusion, in some form, in the work of ICAO entities. The United States supports this objective.

Rule 5 of the Standing Rules of Procedure for the ICAO Assembly declares that "Non-Contracting States and international organizations duly invited by the Council, or by the Assembly itself, to attend a session of the Assembly may be represented by observers." Comprised of 36 Member States (including the United States), the Council is ICAO's governing body that runs the Organization between sessions of the triennial Assembly. The practical question is whether Taiwan can obtain an invitation from the Council or Assembly. The ICAO Council and Assembly both operate by consensus on a matter such as this and, to date, there is no agreement among ICAO Member States on inviting Taiwan to participate as an observer.

Taiwan receives information on ICAO safety, security, and environmental standards and other matters by way of the membership of its airline, China Airlines, in the International Air Transport Association (IATA), which is an active observer in ICAO meetings on behalf of its hundreds of member airlines.

The U.S. Mission to ICAO in Montreal has, and will continue to respond to inquiries for information from Taiwan representatives in Canada about the Organization, to the extent that they seek a better understanding of the structure and rules of procedures of ICAO, including those of the Assembly and the Council.

56838.162

Question#: 7

Topic: profiling

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

Question: The Committee has received a number of letters from organizations representing ethnic minorities that are concerned with the TSA policies that have been implemented post 12/25. Most of these concerns relate to the issue of racial or ethnic profiling by airport screeners.

What measures are being taken to ensure that TSA airport screeners are not engaged in profiling of air travelers on the basis of religion, ethnicity, and national origin?

What kind of instruction have TSA airport screeners received to ensure that civil rights and liberties are protected in the course of enacting enhanced screening measures post-Christmas 2009?

If TSA plans on expanding the use of Whole Body Imaging (WBI) machines, what measures does TSA plan on taking to ensure that use of such machines does not, intentionally or unintentionally, target specific ethnic or religious communities as a form of profiling?

Response: The Transportation Security Administration (TSA) takes a proactive and multi-layered approach to ensuring that unlawful profiling of travelers based on religion, ethnicity, and national origin does not occur. TSA adheres to the "Department of Homeland Security's Commitment to Race Neutrality," a DHS policy document that has been in place since 2004, in security screening programs. TSA neither uses nor condones unlawful profiling in security screening activities. Unlawful profiling is not and has not been an acceptable method of selecting passengers for additional screening.

TSA has mandatory and annual training on both cultural awareness and race neutrality in law enforcement programs for the workforce. Cultural awareness trainings include trainings on the Sikh, Arab, and Muslim cultures. Race neutrality training programs include the Department of Justice's trainings for law enforcement officers to ensure that unlawful profiling does not occur.

In addition to these formal, mandatory courses, TSA provides cultural awareness briefings to the workforce throughout the year on cultural events and religious holidays including Rammadan, Hajj, and Sukkot. For Ramadan, TSA provides awareness to the workforce that observant Muslims may be observed during this month-long holiday

56838.163

Question#: 7

Topic: profiling

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Joseph I. Lieberman

Committee: HOMELAND SECURITY (SENATE)

traveling in groups, praying at the airport, and possibly wearing traditional clothing during travel. This information is important for the workforce to understand because they need to be aware of baseline behaviors and characteristics of the traveling public. For Sukkot, a significant event for persons of the Jewish faith, TSA's standard operating procedures do not prohibit the carrying of the four plants – which include a palm branch, myrtle twigs, willow twigs, and a citron through the airport or the security checkpoints, or on aircraft. These plants are not on TSA's Prohibited Items List. Third, TSA provides cultural awareness briefings for the workforce on Hajj. The training provides awareness that observant Muslims may travel more frequently in groups during this time period, may travel in traditional clothing, may be observed praying more frequently at the airports, and may carry holy water either within or in excess of the 3.1 ounce rule. The briefings provide awareness to the TSOs to respectfully interact with observant Muslims who may carry the holy water in excess of the prescribed quantities and who may need to either check the water or discard the water.

TSA also provides additional briefings to the workforce on a periodic basis advising them of mass movements of people through the checkpoints in a short period of time and the cultural traditions and religious practices they may experience at the checkpoints. In addition, TSA provides periodic briefings to the workforce on handling and screening religious items and artifacts.

TSA continues to assess the measures currently in place, and measures that can be put in place, to strengthen the commitment to race, ethnicity, and religious neutrality in security screening programs. TSA takes a layered approach to ensure that adequate systems are in place to prevent any unlawful profiling. These measures include: workforce accountability, on the job training, cultural awareness training, and civil rights oversight, which includes review of SOP and intelligence products by OCRL personnel who possess the appropriate security clearance.

The Transportation Security Administration (TSA) will continue to assess and evaluate the security initiatives currently in place and security initiatives that can be made operational to strengthen the commitment to race, ethnicity, and religious neutrality in security screening programs, as they relate to Advanced Imaging Technology (AIT). TSA has reached out to multi-cultural coalition members to educate them about AIT and learn about their issues and concerns. TSA has a strong commitment to community engagement. By understanding the concerns of the various communities, TSA will be better able to ensure that the screening methods and technologies do not adversely or unlawfully impact any community.

56838.164

Post-Hearing Questions for the Record
Submitted to Gale D. Rossides
From Senator Claire McCaskill

Question#: 8

Topic: warnings

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Claire McCaskill

Committee: HOMELAND SECURITY (SENATE)

Question: During the hearing, we discussed that the first three warning messages after the failed Northwest Flight 253 on 12/25/09 were sent out only to transatlantic flights. You stated that this was a lesson learned for TSA and that in the future other carriers will be notified. From what I understand, the first three warning messages were sent over two hours after the flight landed and that the broad distribution Security Directive (SD) notification to all airborne and ground crewmembers was sent about seven hours after the flight landed. Coordinated attacks can be seconds and minutes apart. I understand there are investigations required before making the determination to broadcast any warning announcement, but is TSA also looking at processes and procedures for minimizing the time it takes between event occurrences and broadcasting warning communications? Please explain.

Response: The Transportation Security Administration (TSA) strives to ensure its communications during an event are as timely as possible, taking into consideration that every incident is unique and presents its own complicating factors.

The Transportation Security Administration (TSA) strives to ensure its communications during an event are as timely as possible, taking into consideration that every incident is unique and presents its own complicating factors.

In the aftermath of the 12/25 incident, TSA held several working sessions with the FAA, assessing existing operational communications protocols in order to improve incident response and overall performance. These efforts have resulted in positive process change, reflected in the most recent incident (United Airlines Flight 663, occurring on April 7, 2010), when 4,600 aircraft in flight were contacted and provided situational awareness via communications from the Transportation Security Operations Center to the Federal Aviation Administration. TSA would certainly be able to provide a briefing to the Committee regarding these operational improvements.

56838.165

Question#: 9

Topic: information

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Claire McCaskill

Committee: HOMELAND SECURITY (SENATE)

Question: Under Secure Flight, what enforcement mechanisms does TSA have to require airlines to collect the newly required fields for airline travel, both abroad and domestically? What happens if an airline refused to collect this information? What happens if the information is incomplete?

Response: The Transportation Security Administration (TSA) will use the same enforcement process to ensure compliance with Secure Flight requirements that it uses to enforce other TSA security requirements. As a general matter, TSA will open an investigation if an entity fails to comply with TSA's security requirements. Based on that investigation, TSA will decide what type of enforcement action to take. For example, if an aircraft operator is not willing or able to collect Secure Flight Passenger Data (SFPD) according to the Secure Flight Final Rule, codified at 49 C.F.R. part 1560, then TSA would likely conduct an investigation into the noncompliance. Based on the results of the investigation, TSA may decide to take administrative action (e.g. issue a Warning Notice) or impose a monetary civil penalty to deter recurrence of the noncompliance. If TSA determines that any aircraft operator's violations are so egregious that it presents a threat to civil aviation, TSA could suspend service, either by withdrawing TSA approval of the aircraft operator's security program or through an Order, until such time that the threat to civil aviation security is adequately mitigated and the aircraft operator is in full compliance with TSA's security requirements.

56838.166

Question#: 10

Topic: notification

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Claire McCaskill

Committee: HOMELAND SECURITY (SENATE)

Question: If we flagged an individual too late, as we did in the Abdulmutallab case, and the flight departed with a questionable individual on board, what recommendation would you provide with regards to notifying and advising the crew of the particular threat of the passenger while in-fight? Ultimately, we want to be able to catch these individuals before they get on the plane, but if we don't I want to make sure there is proper training and protocols in place to counter the threat with and without a Federal Air Marshall. In this case, given that Abdulmutallab spent 20 minutes in the bathroom prior to igniting the explosive, we might have been able to prevent him from even attempting the act. Would you recommend a requirement to notify the crew of the flight if there is concern about a passenger, such as in the case of the alleged 12/25 bomber?

Response: The Transportation Security Administration (TSA) takes appropriate action when made aware of threat information on aircraft in flight in coordination with our security partners, including contact with the air carriers. The TSA Freedom Center is a 24/7 watch team that is capable of communicating with commercial airlines' Systems Operations Centers that are in contact with the flight deck crewmembers through internal communication systems. This system is capable of communicating both while on the ground and airborne.

In addition to communications with flight crews, TSA has assigned liaison officers who communicate directly with an air carrier's corporate security personnel, both for U.S. aircraft operators (Principal Security Inspectors) and foreign air carriers (International Industry Representatives). These liaison officers are in continuous communication with their assigned air carriers' corporate security personnel and, among other things, would advise them of any threat or other concern so that such information may be immediately disseminated to the affected air carrier's management.

Crewmembers receive annual training in the requirements contained in Vision-100, Century of Aviation Reauthorization Act, philosophy and procedures in Common Strategies, and other subjects deemed necessary by TSA. The training programs include training exercises that simulate threat conditions as noted in the standards. These exercises enable the participants to apply and practice the knowledge acquired during the training to include selecting and executing the appropriate courses of action. Situational training includes various methods of instruction that create an environment or problem requiring a resolution. Examples of situational training include role-playing, simulations, and critical incident techniques. Since flight and cabin crewmembers must effectively work as a team, group-learning activities are encouraged.

56838.167

Question#: 11

Topic: EDS

Hearing: The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening

Primary: The Honorable Claire McCaskill

Committee: HOMELAND SECURITY (SENATE)

Question: My staff attended an FY11 TSA budget overview brief on February 18th and it is my understanding that TSA has used a sole source contract for the procurement of Explosive Detection Systems (EDS) since the beginning of the program several years ago. TSA is now planning to enter into a competitive bidding process by the end of FY10 for EDSs. Is this still the plan? Please provide the updated details.

Response: Yes, the Transportation Security Administration (TSA) will compete the Explosives Detection Systems (EDS) acquisition among those vendors who pass a Qualification Data Package (QDP) validation, certification, and operational testing requirement. Vendors that meet the requirements will be placed on a qualified products list and eligible to compete for future EDS requirements. A synopsis initiating the establishment of a qualified products list was published on www.FBO.gov on January 27, 2010. The next major milestone is submission of QDPs by April 5, 2010. TSA plans to award the contract in January 2011.

56838.168

The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration
Homeland Security and Governmental Affairs Committee
Chairman Joseph I. Lieberman
March 17, 2010

Good morning. Today we continue our Committee's inquiry into the intelligence reforms adopted after 9/11. We do so in the fresh context of the failed terrorist attack on Christmas Day, which exposed continuing gaps in our homeland defenses. Today's hearing – our fourth in the series – will specifically examine the authorities of the Director of National Intelligence (DNI) and the National Counterterrorism Center (NCTC). Our purpose is to determine if those authorities are sufficient or in need of additional reform.

Creation of the DNI and the NCTC were the most critical recommendations made by the 9/11 Commission to improve our ability to protect the American people against the threat of terrorism.

More than five years have passed now since the Intelligence Reform and Terrorist Prevention Act– the so-called 9/11 Commission Act - was signed into law. And that's why, last fall, the Committee began this series of oversight hearings. The Christmas day incident only added urgency to our task and underscored I think how much this is a continuing effort to strengthen our ability to detect and counter potential terrorist threats.

In recent weeks we have held hearings on issues raised by the Christmas day bombing attempt, most recenlty examining our watchlisting and prescreening systems. Next month we're going to hold hearings on our visa issuance procedures and intelligence analysis and information sharing.

But today, as I said, we're going to focus on the DNI and NCTC. We want to consider instances in which these two entities have had difficulty carrying out their intended missions, as well of course the many times they have done exactly what we hoped they would do. We want to discuss also what, if anything, Congress should do to strengthen the abilities of the DNI and NCTC to respond to terrorist and other national security threats, perhaps different threats, that have emerged since 2004.

The 9/11 Commission concluded that no single person or agency was in charge of our sprawling intelligence community and, therefore, recommended creation of the DNI to lead the 16 intelligence agencies of our government – including, of course, the CIA - and to act as the principal advisor to the President on matters of intelligence.

The 9/11 Commission Act gave the DNI a range of authorities to better integrate the intelligence community, to promote what the 9/11 Commission called the "unity of effort" that they found was absent before 9/11.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00363 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.169

The 9/11 Commission further concluded that no one was responsible for coordinating the critical activities of key agencies involved in the fight against terrorism. As the Commission memorably concluded: No one was in charge of the various efforts that had been ongoing to capture or kill Osama Bin Laden. So, the Intelligence Reform Act created the NCTC and gave it the responsibility to conduct a new, but critically important, function in our government, which we called strategic operational planning -- that is, planning counterterrorism activities on a government-wide basis, integrating all elements of our national power to fight terrorism, and assigning roles and responsibilities to Departments and agencies for specific activities, based on that planning.

In many, many instances, the DNI and NCTC have used their authorities very well and implemented critical policies and organizational initiatives to improve intelligence functions and better protect the American people. The NCTC has played a vital role in coordinating federal, state, and local agencies to prevent an ongoing series of terrorist plots against the U.S., including some recent, remarkable acts of prevention in the cases of Najibullah Zazi and David Headley.

But in other instances – such as the case of Umar Farouk Abdulmutallab on Christmas Day - failures have occured. In key areas, progress at fully implementing reforms has been slow – perhaps due to institutional or bureaucratic resistance from some of the 16 agencies that report to the DNI, or perhaps due in other cases to insufficient resources or inadequate leadership. Those are the questions that we want to ask today about where there are the shortcomings and why they have occurred.

I also want to discuss the policy and legal framework for intelligence community information systems. Last week, the Deputy Director of the NCTC testified that policy, legal, and privacy-related barriers impede the development of advanced search and discovery tools that could help analysts spot potential terrorist plots in a way that may have prevented Abdulmutallab from ever boarding Northwest Flight 253. Before 9/11 there was an inability to connect the dots, in part because various intelligence agencies and other agencies of our government were not sharing information and the dots weren't on the same table. I think our feeling now is the dots are on the same table, there is a lot of sharing going on, but there are so many dots on the table that many times it's hard to make connections between them that are necessary. We're focused now on the capacity of technology to assist us in doing that. For humans it's very hard to do that, particularly in a timely way. So I think some of the barriers that were cited last week need to be overcome in the interest of the homeland security of the American people.

I want to thank the three of you, who each bring very relevant and extensive experience to us, for appearing before the Committee and sharing your perspectives on this. I look forward to the discussion after your testimony.

Senator Collins.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00364 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.170

Opening Statement of
Ranking Member Senator Susan M. Collins

"The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration"

Committee on Homeland Security and Governmental Affairs
March 17, 2010

★ ★ ★

Over the past three months, this Committee has examined the intelligence failures surrounding the attempted terrorist attack on Christmas Day. As a part of our due diligence, we also have evaluated the impact of the Intelligence Reform and Terrorism Prevention Act of 2004.

Today, we focus anew on one of the most significant issues that we grappled with in drafting the Intelligence Reform law: the extent of the authority for the Office of the Director of National Intelligence.

The DNI was established to be, in Colin Powell's memorable words, the "quarterback" of the intelligence community, to coordinate the activities of the 16 intelligence agencies scattered across the federal government. Those 16 diverse components carry out an array of missions, each with its own view about how best to carry out its assignment.

The intelligence community is resistant to change, but change is precisely what the Intelligence Reform Act directed the DNI to achieve. To that end, we provided a set of authorities that the DNI would use as tools to encourage, cajole, and, in some cases, compel action.

These authorities included:

- The ability to access all intelligence information collected by the federal government.
- The lead role in developing the annual National Intelligence Program budget and ensuring its effective execution.
- Some ability to transfer funds and personnel within the Intelligence Community.
- The ability to manage and direct the tasking, collection, analysis, production, and dissemination of intelligence.
- The authority to develop standards and guidelines to ensure maximum availability of intelligence information within the Intelligence Community.

56838.171

These authorities should be sufficient for the DNI to accomplish its mission - provided they are wielded effectively and with the strong support of the President. As Governor Kean and Representative Hamilton testified before this Committee in January, "The DNI's ability to lead the Intelligence Community depends on the President defining its role and giving him the power and authority to act."

The question is, however, whether or not these authorities have been used as often and in the manner intended by this Congress.

Does the institutional resistance of agencies like the CIA make use of these authorities such an onerous ordeal that the DNI is hesitant to embark upon this journey?

Is the DNI concerned that exercising these authorities more aggressively might create ill will that will make it even more difficult to coordinate activities in other areas?

Or, are these authorities being undercut by insufficient support from the President or the National Security Council, both of which need to be active to ensure that the DNI works as intended?

Our witnesses today offer a wealth of practical experience in the day-to-day operations of the Intelligence Community both pre- and post-reform, and I hope that they can offer some insight into these questions.

56838.172

STATEMENT OF BENJAMIN A. POWELL BEFORE THE SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

"The Lessons and Implications of the Christmas Day Attack: Intelligence Reform and Interagency Integration"

MARCH 17, 2010

Introduction

I appreciate the opportunity to appear before the Committee to discuss intelligence reform and interagency integration. I am particularly honored to appear before this Committee given the historic role in intelligence reform played by this Committee, under the leadership of Senator Lieberman and Senator Collins, in the crafting of the most significant changes to the Intelligence Community (IC) since the enactment of the National Security Act of 1947.

I appear before the Committee in my personal capacity and the views I express are my own. None of the views expressed in this statement or in my discussions with the Committee should be understood in any way to reflect the views of my employer. This statement was reviewed by the government for classification purposes.

I have separately provided the Committee my biography. I have been involved in information sharing and data handling issues related to the IC going back to the late 1980s in work at the Federal Bureau of Investigation (FBI) and as an officer in the Air Force prior to becoming an attorney. I was involved in the formation and drafting of the various proposals for intelligence reform that ultimately resulted in the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). As an Associate Counsel to the President and Special Assistant to the President, I spent a significant amount of my time on intelligence transformation issues, reviewing and responding to the recommendations of the 9/11 Commission related to intelligence transformation, and assisting in the drafting and interagency coordination of directives related to the IC. Of course, the most significant change to the IC was the legislative direction contained in the IRTPA.

As General Counsel for the first three Directors of National Intelligence, I have seen the implementation of the IRTPA at the ground level. From my perspective, a substantial amount of the actual details of transformation – both good and bad – has been obscured at times by a fog of commentary not always grounded in law, fact, or actual experience. The work of transformation at its ground level is often in the less glamorous areas of policy directives, implementation of standards, and oversight to ensure there is actual implementation and measurement of the success or failure of policy changes. And while it can appear quite distant from the daily operational activity of the IC, the 9/11 attacks and subsequent events have made clear that this is work with real world consequences. The Christmas Day attack was another vivid example of the importance of an integrated IC. Neglect in building an integrated IC will have negative consequences for the Nation.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00367 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.173

IC transformation is not a zero sum project. The goal is not to diminish the authorities or capabilities of one organization in favor of another organization, such as the DNI's office. The goal is to have an integrated IC that is more than the sum of its parts and has greater capabilities to confront serious global threats.

Support from this Committee, the Senate Select Committee on Intelligence, and senior congressional leaders for the efforts to build a more integrated and capable IC has been critical to the ability of the DNI and IC to implement the mandates of the IRTPA and other legislation. I hope that current and future leaders of the IC continue to receive support and leadership from the Congress on these issues.

DNI Leadership

This Committee is well aware of the lengthy list of responsibilities given to the DNI to lead the IC and improve its operations. The IRTPA did not create a Department of Intelligence that combines all intelligence elements under a single leader with complete direction, control, and authority. Instead, for a number of reasons, the IRTPA created a structure of matrix management, providing the DNI with responsibilities and authorities in certain areas, while leaving other duties with heads of departments containing elements of the IC. An organization chart for the IC is attached at Annex 1.

Some observers have argued that the IRTPA is filled with ambiguity and a lack of clarity, leaving the DNI with an unclear mission and little authority to carry out the mandate of the IRTPA. I think that conclusion sweeps too broadly. The legislation is not free from ambiguity, but significant legislation often entails compromise and leaves areas unclear for further definition in implementation of the statute.

Section 102A of the National Security Act of 1947, as amended, provides a lengthy list of DNI responsibilities and authorities. Section 102A is codified at 50 U.S.C. § 403-1 and attached at Annex 3 to this statement. Certainly, the responsibilities are more clear than the authorities provided to meet the mandates contained in the legislation. Thus, the DNI's office spent significant amounts of time working with elements of the IC to interpret the IRTPA and determine how the DNI's authorities can be exercised to meet the DNI's assigned responsibilities. Many of these discussions, whether over information sharing, personnel policies, budget authority, collection priorities, or other areas, seemed to be less legal at their core and more in fact discussions of the policy, cultural, and organizational change issues created by the integration demanded by the Congress and President in the IRTPA.

One overlooked benefit of the creation of the DNI is the critical value in having a leader and an organization that was not connected to a particular agency and could serve as an "honest broker" over disputes or provide greater visibility at senior intelligence levels to serious problems impacting a single IC element. I saw significant interagency national security issues come before the DNI, senior officials, or the Executive Committee (EXCOM) for discussion and resolution. In addition, IC elements in individual departments may have significant intelligence challenges that do not receive adequate attention as they compete for attention with many other non-intelligence related issues facing a department head. The DNI could concentrate on these

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00368 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.174

intelligence issues and ensure they received appropriate attention in the DNI's office, the National Security Council, or other organizations.

The IRTPA omits some authorities that would provide greater control to the DNI. First, as Secretary Gates has pointed out, the DNI does not have hiring or firing authority for the heads of most of the elements of the IC. Recent examples outside the IC have shown the importance of a department head being able to exercise this blunt instrument when the department head has determined that a subordinate is pursuing a course different from the department head or not satisfactorily meeting expectations. Revisions to Executive Order 12333 went beyond the IRTPA in providing additional authority for the DNI in this area. Currently, the DNI is generally provided input into hiring and firing for most leaders of the IC, but must negotiate and work with other leaders to effect any leadership changes.

Second, the diverse nature of the IC, with a personnel mix that ranges from the uniformed military to CIA officers to FBI agents to State Department professionals, located in departments and agencies governed by a range of laws and regulations provides an especially difficult challenge to the implementation of uniform policies in areas such as information sharing and joint duty. The IRTPA mandated joint duty, increased information sharing, uniform security policies, and many other important standards and policies. But harmonizing these mandates with the laws and regulations governing these areas in each department required careful review and discussion with each department. For example, as discussed more below, joint duty policies took years to implement as the DNI's office worked with each department to determine how an IC-wide policy would impact their individual compensation, assignment, evaluation, and promotion system.

The IRTPA sets up a challenging matrix structure of shared control over the IC. As I discuss below, the DNI has made significant progress on many issues since 2004 and the current structure, for all its challenges, can pursue meaningful improvements for the security of the Nation. As Congress considers future legislation related to the DNI, it may find it useful to examine laws governing information sharing, privacy, personnel and other areas and determine the best way to harmonize these laws governing individual departments with the mandates of the IRTPA to create a more integrated IC. But the success of the DNI will not solely be determined by the clarity of the IRTPA or subsequent legislation.

The support of the President, his senior national security team, and the Congress is critical to building a unified national intelligence enterprise. I should note one "foundation" myth related to the former President's support that has become conventional wisdom, but is contrary to my experience. I have heard many people comment that former President Bush only accepted the IRTPA and the creation of the DNI because of the pending 2004 election. I am not aware of evidence to support this assertion. First, the fundamental fact is that the IRTPA was not passed in the House and Senate until December 2004, after the 2004 election, and not signed until December 17, 2004. The most difficult negotiations from my perspective took place also after the 2004 election. Second, I believe the President would not have personally become involved in urging passage of the legislation and working with the Congress after the 2004 election if the President did not support the legislation. Third, every interaction I had with former President Bush after the election indicated that he wanted the legislation and wanted a

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00369 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.175

strong DNI. And his actions in supporting the DNI after the enactment of IRTPA reflected his support for a strong DNI who vigorously exercised the DNI's authorities and brought greater integration to the IC. His support for and direct involvement in the revision of Executive Order 12333 is further evidence of his views on a strong DNI.

Fundamentally, the DNI will succeed if the President and the National Security Council, with the support of Congress, provide backing for the DNI's leadership of the IC and demand integration and transformation. Absent that support, transforming our IC into the integrated Community needed to deal with the current and future threats of the 21st Century will not happen.

This is not a new insight. The members of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("Silberman-Robb Commission") – members with many decades of national security experience – made this point in its submission to former President Bush in 2005, where they stated:

> **Give the DNI powers--and backing-to match his responsibilities.**
>
> In your public statement accompanying the announcement of Ambassador Negroponte's nomination as Director of National Intelligence (DNI), you have already moved in this direction. The new intelligence law makes the DNI responsible for integrating the 15 [now 16] independent members of the Intelligence Community. But it gives him powers that are only relatively broader than before. The DNI cannot make this work unless he takes his legal authorities over budget, programs, personnel, and priorities to the limit. It won't be easy to provide this leadership to the intelligence components of the Defense Department, or to the CIA. They are some of the government's most headstrong agencies. Sooner or later, they will try to run around---or over-the DNI. Then, only your determined backing will convince them that we cannot return to the old ways.

Transmittal Letter from Silberman-Robb Commission to the President (March 31, 2005) at p. 2, *available at* http://www.gpoaccess.gov/wmd/pdf/full_wmd_report.pdf. The Commission consisted of: Charles Robb, Judge Laurence Silberman, Richard Levin, Sen. John McCain, Henry Rowen, Walter Slocombe, Admiral William Studeman, Charles Vest, Judge Patricia Wald, Lloyd Cutler (of counsel), and Vice Admiral John Scott Redd (Executive Director). The same points were forcefully made by former Congressman Lee Hamilton and former Governor Tom Kean in testimony before this Committee on January 26, 2010, where they stated:

> Is the DNI a strong leader of the intelligence community empowered to lead the IC as an enterprise? Or is the DNI a mere coordinator, a convening authority charged with helping facilitate common inter-intelligence agency agreement? The lack of settled clarity on its mission invites a host of other criticisms, including that the ODNI is too large, too intrusive, and too operational.
>
> The burden is on the President to be clear on who is in charge of the Intelligence Community and where final authority lies on budget, personnel, and other matters. In our estimation, we need a strong DNI who is a leader of the intelligence community. The

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00370 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.176

> DNI must be the person who drives inter-agency coordination and integration. At the same time, the DNI's authorities must be exercised with discretion and consideration of the priorities and sensitivities of other intelligence agencies. But the President's leadership is crucial and must be continuing or we run the risk of mission confusion and decrease the prospect of long and lasting reform that was recommended after September 11, 2001. The DNI's ability to lead the Intelligence Community depends on the President defining is role and giving him the power and authority to act.

Hearing on Intelligence Reform: The Lessons and Implications of the Christmas Day Attack, Part II Before the S. Homeland Sec. Comm., 111th Cong. (2010) (statement of Congressman Lee Hamilton and Governor Tom Kean) at p. 5, *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=756c2ecd-328f-4efd-849e-27ce8f348acd (emphasis in original). Presidential-level support, combined with support from the President's national security team, is needed to continue with ensuring our IC is ready to confront the global threats facing the country now and in the future.

Integration and Transformation

The DNI structure has been challenged over its mission, size, and roles from even before the enactment of the IRTPA. A significant part of this discussion may result from continued dissatisfaction with the IRTPA, and not particular initiatives pursued by the DNI. There is no doubt that changing the prior Director of Central Intelligence structure and creating a DNI with a full-time mission of overseeing the IC and a mandate to bring greater integration across the IC was a seismic shift. Change of this magnitude takes many years to fully implement and remains a work in progress. A debate over structure is quite appropriate and the IRTPA can always be reconsidered by Congress and the President. However, using such a debate to hobble needed progress on intelligence reform within the current structure is corrosive to the IC mission and needed progress on transformation.

The DNI has exercised authority in many areas with varying levels of success over the past five years. As I mentioned before, critical work on many of these initiatives was also done by other departments and agencies. The DNI was not acting alone on these initiatives. However, the DNI's office was frequently a necessary leader or participant in initiatives that required teamwork across the IC. Some of the larger initiatives included:

- Working with Congress to enact fundamental change to the Foreign Intelligence Surveillance Act of 1978 (FISA) to modernize FISA and significantly improve our foreign intelligence collection activities.
- Supporting the standup of the National Counterterrorism Center (NCTC) and its ability to access relevant information across the government.
- Implementation of Joint Duty.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00371 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.177

- Working with the President to update Executive Order 12333, the foundational Executive Order governing the IC, to clarify and align DNI and IC authorities and reflect the many changes in the IC since the order was signed in 1981.

- Security clearance reform

- Deployment of technologies in innovative ways such as the Analytic Space (A-Space), Intellipedia, and other information technology systems.

- Critical work in the cyber area that culminated in the Comprehensive National Cybersecurity Initiative (CNCI).

There are many other important areas where the DNI exercised authorities including reprogramming of funds to deal with higher priority issues, identifying gaps in our understanding of threats to the Nation, setting collection and analysis priorities, and supporting the mission and support activities for the IC. I also omit important classified work that consumed significant resources and time of senior officials from the DNI's office.

Some observers have claimed that the IRTPA and the DNI's subsequent implementation merely added a "new layer of bureaucracy" and accomplished little. That does not reflect the reality of the past five years.

For example, deficiencies in FISA were known since at least 1990. Many reasons account for a failure to confront defects in the statute that put the Nation at risk and became worse with greater changes in communication technology. Without a DNI working this issue night and day, and providing the strong push to seek legislative change, FISA legislation would not have been enacted, serious collection gaps would remain (and would have worsened), and the Nation would face greater risk.

The pre-IRTPA structure did not have a single person who could have committed the resources or the level of individual commitment to getting such a significant change enacted into law. Indeed, we can only speculate as to how history would have changed if a DNI existed in 2001 or in earlier years. As with all these initiatives, the DNI's office depended on the support from leaders and professionals across the IC and other departments and the Congress. The DNI's office was not sufficient alone to get the changes enacted, but it was necessary, as were the other participants, for the ultimate outcome.

The DNI received some criticism for its involvement in asking for legislative changes to improve IC operations. I firmly believe that the IRTPA mandates that the DNI put forth suggestions for change when the DNI identifies an inadequacy in existing law. Also, an additional advantage of having a DNI leading the IC was that IC element heads were more insulated from the public controversy surrounding the FISA legislation, and the political nature of the debate at times, and could concentrate on their important operational day-to-day work of running their agencies.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00372 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.178

NCTC has been the subject of recent hearings of this Committee and I will only discuss NCTC briefly. NCTC has "collocate[d] more than 30 intelligence, military, law enforcement and homeland security networks under one roof to facilitate robust information sharing" and has access to a variety of databases. *See* National Counterterrorism Center: About Us, http://www.nctc.gov/about_us/about_nctc.html (last visited Mar. 15, 2010). Gaining access to information sources across the government is a detailed task requiring that personnel work through a web of laws, regulations, and guidelines governing the use and distribution of each particular type of information. Without the DNI structure, I am unsure where a NCTC organization could effectively reside or find the support to work through information sharing challenges. Because of its organizational location apart from particular operational elements, NCTC sits in a unique position apart from individual IC elements and is able to access a broader variety of information. The legal, policy, and other issues created by locating NCTC in an element of the IC would be very complex and probably unworkable without significant legal and organizational changes.

Joint duty is critical and its implementation will be a long-term project. *See* Intelligence Community Directive No. 601, Human Capital Joint Intelligence Community Duty Assignments (May 16, 2006) and Intelligence Community Policy Guidance 601.1, Civilian Joint Duty Program Implementing Instructions (As Amended Sept. 4, 2009), *available at* http://www.dni.gov/electronic_reading_room.htm. The signing of the Joint Duty Directive and its accompanying implementation guidance took years and is a practical example of many of the issues discussed in this statement. First, the DNI's office needed to gain an understanding of the wide variety of personnel systems both within IC elements and across departments. This knowledge was not sitting on a shelf in any particular agency. Second, the DNI could not just sign a directive implementing joint duty. Signing a directive without extensive discussions with the IC elements and departments would have been both unwise and resulted in a policy that would likely be ignored. The discussions and negotiations over joint duty were not the result of resistance in the IC to the idea of joint duty or a desire to avoid the legislative mandate. IC elements wanted to ensure their particular evaluation, assignment, promotion, pay, and other personnel processes could be harmonized with an IC-wide personnel policy. We also had to work through issues related to legal authorities and how they would apply in practice to items such as the granting of exemptions of positions from joint duty requirements, designation of joint duty positions, tracking of promotion rates, and waivers of joint duty requirements for individuals. Smaller elements of the IC had to determine how to incorporate new personnel policies and processes relating to a single office in a much larger department that was not adopting those policies and processes, without creating unworkable internal inconsistencies. This is just a few of the issues that the DNI's office and the IC needed to work through on this policy.

Joint duty is an example of the investment of time and effort required to formulate and implement workable policies in the IC's structure of matrix management. This effort required dedicated personnel in the DNI's office working through issues with the agencies, large data collection efforts, coordination with sixteen IC elements, and obtaining agreement across the senior leaders of the IC. I have strong doubts that the pre-IRTPA structure could have produced an IC-wide initiative of this scope and complexity. The joint duty experience does suggest that

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00373 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.179

future legislation related to the DNI should consider how the responsibilities assigned to the DNI will interact with other laws and regulations governing the various IC elements and their respective departments.

Many other initiatives were pursued since the passage of IRTPA. Executive Order 12333 required modification for many years. A number of past attempts to update the Executive Order were unsuccessful. The DNI was able to make revision of this Executive Order a priority and identify deficiencies in the existing Order. Significant parts of the Order parallel the mandates contained in IRTPA, but there are important provisions in the Order enhancing the DNI's authority, clarifying roles between the agencies (particularly in the domestic and foreign spheres of operation), and aligning the missions of IC elements. The amended Executive Order 12333 is attached at Annex 4.

Security clearance reform has been the subject of much discussion and dissatisfaction for decades. This area has been a particular focus of this Committee's Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia under the leadership of Senator Akaka and Senator Voinovich. The cost and delays present in the process impose a large cost on the IC. In response to the mandates contained in the IRTPA, the DNI used his authorities to join with the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), the Department of Defense (DoD), and other agencies to carry out pilot projects and explore the use of technology to bring down the cost and timeframes associated with clearances. This must be done very carefully because of counterintelligence issues, but significant progress continues to be made in this area. In November 2005, Top Secret investigations took an average of 314 days to complete with only 8 percent being completed within 90 days. I understand that currently, 90 percent are completed within an average of 91 days. In November 2005, Secret and Confidential investigations took an average of 153 days, with just 44 percent completed within 90 days. I understand that currently 90 percent are completed within 49 days. I also understand that the decades-old backlog of investigations, which as recently as October 2006 stood at almost 100,000 cases, has been eliminated. In addition, I understand that the government, with an IC-led effort, believes it will substantially reach its goal by December 2010 of having an end-to-end e-service security clearance process in partnership with OMB, OPM, and DoD that will lead to US Government-wide benefits.

The deployment under the DNI's guidance of A-Space and other collaborative tools are innovative technologies that significantly improve the analytical capability of the IC. They also threaten old ways of doing business that unnecessarily prevent collaboration and will challenge unneeded bureaucratic policies. The IC is a young workforce familiar with social networking and other tools. These technologies will facilitate collaboration across organizational boundaries and will challenge existing organizational structures. On balance, that is a positive development for the Community, but the DNI's analytic and counterintelligence team will need to monitor these efforts to ensure accurate information is the end result of the collaboration and security is not compromised. The differing legal regimes governing the sharing of information may also prevent the full use of these technologies and present unanticipated challenges in implementation.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00374 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.180

Without the DNI's office, the Nation would not have a CNCI and be less prepared for the cyber threat that Director Blair recently discussed in testimony to Congress. Much of the discussion in the Administration and Congress to address cyber threats was a direct result of the intense focus on the issue by the DNI organization.

* * *

My purpose in this brief and necessarily incomplete discussion of DNI initiatives is an attempt to bring greater clarity to the discussion of the mission of the DNI and the associated responsibilities and authorities. There are ample grounds for debate as to the proper policies and operations of the IC in all of these areas, from personnel policy to operational roles to required legislation. There is opposition to FISA reform, there was significant criticism of the formation of NCTC, and virtually every other initiative of any significance has been the subject of much constructive criticism. But instead of fairly meaningless charges of "another layer of bureaucracy," I would hope the questions would focus on substance, such as:

- Are these IC initiatives useful efforts? Which initiatives should be pursued and how? Do they make the IC better integrated and ultimately produce better intelligence?
- Who should pursue these initiatives? If a dedicated DNI staff is not the proper place or structure, what structure should pursue these initiatives and what is the feasibility of that structure and staffing?
- Historically, how did alternative structures perform? Did they produce the needed integration and transformation of the IC?

Depending on the answers to these questions, the Administration and Congress can work with the DNI to determine the best allocation of time and resources.. If there is a better structure to create an integrated, agile, and capable IC for the 21st Century, I would hope that such a structure will be pursued with the greatest urgency.

Size of DNI Office

Director Blair has talked about the DNI's responsibilities for guiding a "200,000 person, $75 billion national enterprise in intelligence, whose job is to help our policymakers, to support our troops and diplomats in the field and to build better tools and a better workforce so that we can do the job even better in the future." Media Conference Call with the Director of National Intelligence, Mr. Dennis C. Blair (Sept. 15, 2009), http://www.dni.gov/interviews/20090915_interview.pdf. Given the effort spent on the charges and counter-charges concerning the size of the DNI over the years, I would be remiss if I did not discuss this issue. Significant parts of the criticism may be based on fundamental disagreement with the creation of the DNI and a dedicated staff performing oversight and policy functions IC-wide. They may also reflect disagreements with the manner in which the DNI's office carries out its functions.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00375 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.181

First, some facts about the size of the core DNI staff. This core staff consists of individuals carrying out, among other tasks, the DNI's responsibilities to oversee the budget, develop policies, plans, and requirements, oversee acquisition and technology issues, and oversee analytical and collection efforts. In addition, there are functions related to human capital initiatives, a legislative office that in the first 12 months of the DNI's standup supported approximately 660 congressional briefings and meetings with Congress and appearances by the DNI's office at 43 hearings before 13 congressional committees, Chief Information Officer functions, Civil Liberties and Protection, General Counsel, Inspector General, and other functions. *See* Remarks to the ABA Standing Committee on Law and National Security (June 22, 2006), http://www.dni.gov/speeches/printer_friendly/20060622_speech_print.htm. A number of these functions were mandated by the IRTPA and in fact substantial portions of the staff consist of individuals transferred into the DNI's office pursuant to the IRTPA. In addition, there are the support functions that are required of any agency of the government, ranging from responding to Freedom of Information Act (FOIA) requests to EEO to infrastructure issues.

As of January 2009, Director McConnell spoke about a core group of intelligence professionals of 650. *See* Media Roundtable with Mr. Mike McConnell, Director of National Intelligence (Jan. 16, 2009), http://www.dni.gov/interviews/20090116_interview.pdf. As he noted in his discussion, the larger numbers often used to describe the size of the staff include the centers and other support activities for the IC as detailed on Annex 2. For example, NCTC "is staffed by more than 500 personnel from more than 16 departments and agencies (approximately 60 percent of whom are detailed to NCTC)." *See* National Counterterrorism Center: About Us, http://www.nctc.gov/about_us/about_nctc.html (last visited Mar. 15, 2010).

Under any method of calculation, the DNI is a very small proportion of the entire IC population. I understand that the IC is managed with a staff smaller than staffs of DOD's regional combatant commands or, as Director Negroponte has pointed out, the U.S. embassies in the Philippines, Mexico, or Iraq. (I am not including contractors in these numbers as I am not aware of unclassified figures concerning contractors.)

Second, the DNI is given a lengthy list of mandates and responsibilities in IRTPA, subsequent legislation, and Executive Order 12333. *See, e.g.*, Annexes 3 and 4. If those responsibilities are unnecessary or properly belong elsewhere, then those responsibilities, along with staff, should be changed and removed from the DNI's already lengthy "to do" list. I have also heard claims that the DNI was not what was "envisioned" or its "growth" was too rapid (despite the fact that such growth was often the result of the transfer of pre-existing staff and functions to the DNI). At the same time, the DNI was often criticized for not improving information sharing fast enough, not fixing acquisition issues quicker, and a host of other open action items.

Those who work in the DNI's office are working according to what the law states in the IRTPA, subsequent legislation, and Executive Order 12333. When those responsibilities are matched up against the needed staffing, I do not think the size of the DNI seems significantly out of proportion. Some have suggested that perhaps the DNI could just order a lead agency to carry out his responsibilities and therefore have little staff. I do not think such a process would be practical or have a realistic chance of success given concerns that the lead agency may "tilt" the

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00376 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.182

playing field to their advantage or the lead agency may have other immediate priorities that overshadow its IC responsibilities.

Third, perhaps the proper size of the staff is larger or smaller than the 650 persons that Director McConnell discussed in January 2009. I am sure, as with most organizations in government, that there are many efficiencies and improvements in staffing that require examination. The DNI's office has not been perfect in its staffing or in every interaction with the IC or other departments and agencies. But the debate of whether the right number of personnel is 475, 592, 725 or some other number pales in significance next to the questions concerning information sharing, collection requirements, multi-billion dollar acquisition program oversight, analytical excellence, and a host of other issues on the DNI's list of responsibilities. And of course, the delta in terms of numbers is insignificant compared to the amount of time and effort spent on this issue.

Finally, the fact is the DNI cannot issue directives and walk away expecting that they will be carried out. The structure set up by IRTPA demands extensive interagency consultation and careful crafting of IC-wide policies. The DNI must monitor implementation and results, particularly in a matrix management structure where bureaucratic drift is all but inevitable.

Ultimately, much of the debate over the DNI may reflect fundamental disagreement with a strong DNI or a different vision of a DNI with little power to develop complex policies and oversee their implementation. Given the size and budget of the IC, it is difficult to see a radically different staffing situation without fundamental changes to the responsibilities or operation of the DNI.

Conclusion

Implementation of the matrix management structure created by IRTPA has presented numerous challenges. But failing to act on intelligence transformation was unacceptable and pursuing alternative structures would have also led to significant challenges. Significant progress has been made through the exercise of DNI's authorities. Many tasks remain undone and progress on building an integrated, innovative, and more effective IC is likely to be uneven in the coming years. Continued attention on these issues and support for the effort from the President, the Congress, and senior national security officials is vital if the DNI is to successfully lead the IC in the 21st Century.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00377 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

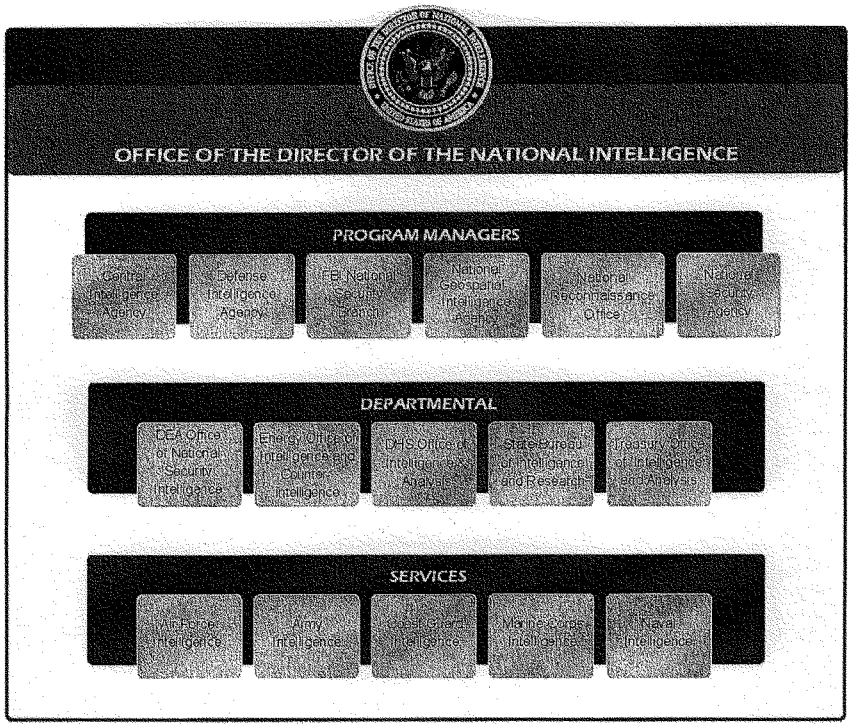
56838.183

ANNEX 1

Elements of the U.S. Intelligence Community

56838.184

U.S. INTELLIGENCE COMMUNITY

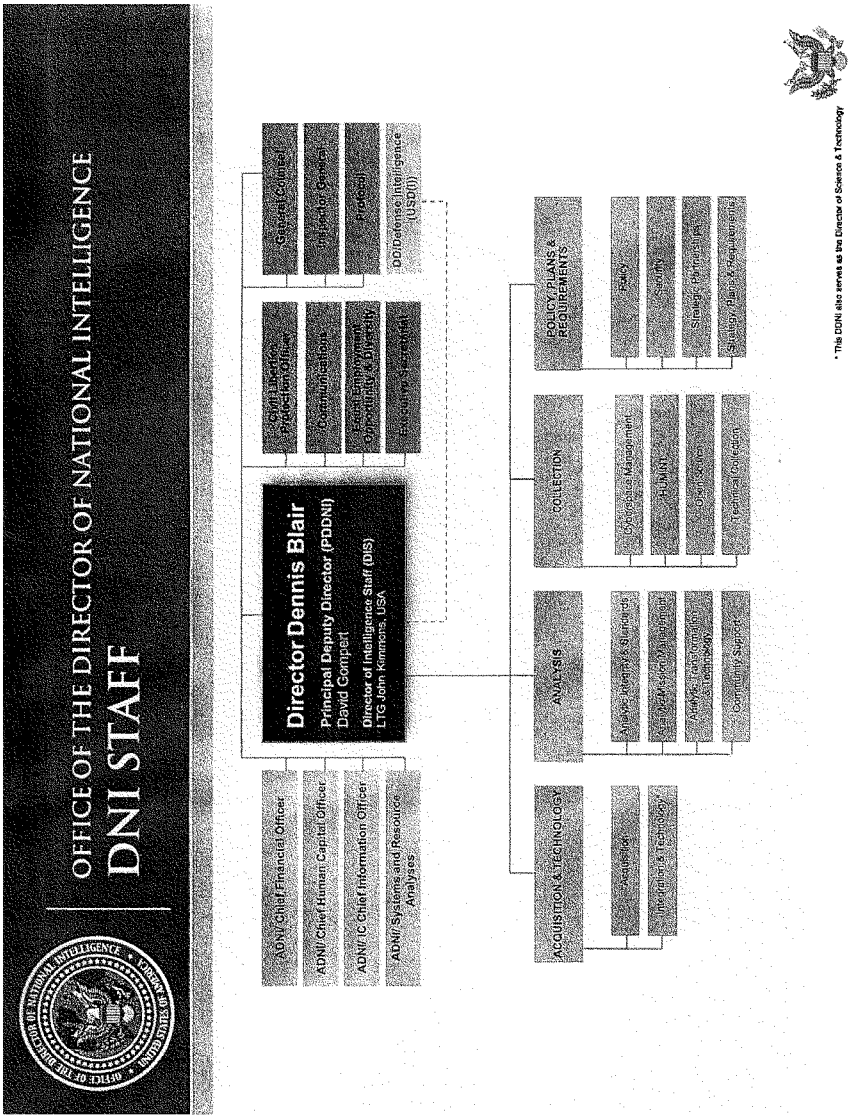


ANNEX 2

Organizational Chart

Office of the Director of National Intelligence

56838.186


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DNI STAFF
ADNI/ Chief Financial Officer
ADNI/ Chief Human Capital Officer
ADNI/ IC Chief Information Officer
ADNI/ Systems and Resource Analyses
Director Dennis Blair
Principal Deputy Director (PDDNI)
David Gompert
Director of Intelligence Staff (DIS)
LTG John Kimmons, USA
Civil Liberties Protection Officer
Communications
Equal Employment Opportunity & Diversity
Executive Secretariat
General Counsel
Inspector General
Protocol
DD/Defense Intelligence (USD(I))
ACQUISITION & TECHNOLOGY
Acquisition
Information & Technology
ANALYSIS
Analyse Intelligence Standards
Lead DNI Analytic Mission
Analytic Transformation & Technology
Community Support
COLLECTION
Collection Management
HUMINT
Open Source
Technical Collection
POLICY, PLANS & REQUIREMENTS*
Policy
Security
Strategic Partnerships
Strategy, Plans & Requirements
* The DDNI also serves as the Director of Science & Technology

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
MISSION AND SUPPORT ACTIVITIES FOR THE IC

BUSINESS TRANSFORMATION OFFICE (BTO)
Catalyst for transforming the IC into an efficient and effective Intelligence Enterprise with standardized common business practices, including human resources and financial management processes. *Established under the DNI in October 2008.*

CENTER FOR SECURITY EVALUATION
Joint State Dept./DNI office protecting intelligence sources and methods information at US diplomatic facilities abroad. *Established in 1988 as a DCI Center. Realigned under the DNI in April 2005.*

INFORMATION SHARING ENVIRONMENT
Establishes a trusted partnership and culture of information sharing between federal departments and agencies and state, local and tribal governments, the private sector, and foreign partners to ensure multi-directional sharing of information. *Established in 2005 in accordance with IRTPA. Realigned under the DNI in 2007.*

INTELLIGENCE ADVANCED RESEARCH PROJECTS ACTIVITY (IARPA)
Invests in high-risk/high-payoff research that has the potential to provide our nation with an overwhelming intelligence advantage over future adversaries. *Established in 2007 with existing components from NSA and CIA.*

INTELLIGENCE TODAY OFFICE
Produces a single centralized website allowing customers to access the IC's most timely analytic insights in support of key national security decisions. Designed specifically for senior policymakers who do not receive the PDB. *Established under the DNI in 2009.*

MISSION SUPPORT CENTER
Provides centralized administrative support for ODNI Mission & Support activities, including infrastructure and personnel support services. *Established under the DNI in 2008.*

MISSION MANAGEMENT TEAMS (COUNTRY SPECIFIC)
Integrates all collection and analysis on priority intelligence topics across IC. Teams include Iran, North Korea, Cuba/Venezuela, and Afghanistan/Pakistan. *Created in November 2005 upon recommendation by the WMD Commission in its 2005 report. Af-Pak team added in 2009.*

NATIONAL INTELLIGENCE UNIVERSITY (NIU)
Oversees and integrates IC education and training, including foreign language training and policy. *Established in 2005 under the DNI.*

NATIONAL COUNTERTERRORISM CENTER (NCTC)
Nation's primary organization for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism. *Previously the Terrorist Threat Integration Center (TTIC), which was managed by the DCI and began operations in May 2003. Realigned under the DNI as NCTC in 2005.*

NATIONAL COUNTERINTELLIGENCE EXECUTIVE (NCIX)
Head of national counterintelligence for the US Government. Provides a counterintelligence (CI) perspective in all IC support to policy makers and departments and agencies outside the IC. *Created in 2001 under the DCI. Realigned under the DNI in April 2005 in accordance with IRTPA.*

NATIONAL COUNTERPROLIFERATION CENTER (NCPC)
IC center for all US Government efforts to discourage, eliminate or counter current and future threats from biological, chemical, nuclear, and radiological weapons. *Created under the DNI in November 2005 as recommended by the WMD Commission in 2005.*

NATIONAL INTELLIGENCE COORDINATION CENTER (NIC-C)
Nation's primary mechanism for the coordination, assessment, and efficient utilization of the total array of U.S. intelligence collection capabilities and resources. Co-located with the Defense Intelligence Operation Coordination Center. *Established in 2007.*

NATIONAL INTELLIGENCE COUNCIL (NIC)
Leads and coordinates analysis across the IC, represents IC analytic views to the policy community, and directs National Intelligence Estimates and other mid-term and long-term strategic analyses. *Formed under the DCI in 1979. Realigned under the DNI in 2005.*

PRESIDENT'S DAILY BRIEFING (PDB) STAFF
Manages the production and delivery of daily intelligence presentations for the President and select administration seniors. *The most recent of several formats and names since the Truman era. The creation of the ODNI moved senior authority for this presidential support from CIA to DNI in 2005.*

SPECIAL SECURITY CENTER
Leads security clearance transformation and assists the DNI in sharing and protecting national intelligence information, creating standard security procedures and managing controlled access programs. *Previously the Director's Special Security Center under the DCI. Realigned under the DNI in 2005.*

ANNEX 3

Section 102A of the National Security Act of 1947

Codified at 50 U.S.C. § 403-1

56838.189

"(1) the Permanent Select Committee on Intelligence and the Committee on Armed Services of the House of Representatives; and

"(2) the Select Committee on Intelligence and the Committee on Armed Services of the Senate."

CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Pub. L. 88-643, Oct. 13, 1964, 78 Stat. 1043, as amended by Pub. L. 90-539, Sept. 30, 1968, 82 Stat. 902; Pub. L. 91-185, Dec. 30, 1969, 83 Stat. 847; Pub. L. 91-626, §§1-6, Dec. 31, 1970, 84 Stat. 1872-1874; Pub. L. 93-31, May 8, 1973, 87 Stat. 65; Pub. L. 93-210, §1(a), Dec. 28, 1973, 87 Stat. 908; Pub. L. 94-361, title VIII, §801(b), July 14, 1976, 90 Stat. 929; Pub. L. 94-522, title I, §§101, 102, title II, §§201-213, Oct. 17, 1976, 90 Stat. 2467-2471; Ex. Ord. No. 12273, Jan. 16, 1981, 46 F.R. 5854; Ex. Ord. No. 12326, Sept. 30, 1981, 46 F.R. 48889; Pub. L. 97-269, title VI, §§602-611, Sept. 27, 1982, 96 Stat. 1145-1148, 1152-1153; Ex. Ord. No. 12443, Sept. 27, 1983, 48 F.R. 44751; Ex. Ord. No. 12485, July 13, 1984, 49 F.R. 28827; Pub. L. 98-618, title III, §302, Nov. 8, 1984, 98 Stat. 3300; Pub. L. 99-169, title VII, §702, Dec. 4, 1985, 99 Stat. 1008; Pub. L. 99-335, title V, §§501-506, June 6, 1986, 100 Stat. 622-624; Pub. L. 99-514, §2, Oct. 22, 1986, 100 Stat. 2095; Pub. L. 99-569, title III, §302(a), Oct. 27, 1986, 100 Stat. 3192; Pub. L. 100-178, title IV, §§401(a), 402(a), (b)(1), (2), Dec. 2, 1987, 101 Stat. 1012-1014; Pub. L. 100-453, title III, §302(a), (b)(1), (c)(1), (d)(1), (2), title V, §502, Sept. 29, 1988, 102 Stat. 1906, 1907, 1909; Pub. L. 101-193, title III, §§302-304(a), 307(b), Nov. 30, 1989, 103 Stat. 1703, 1707; Pub. L. 102-83, §5(c)(2), Aug. 6, 1991, 105 Stat. 406; Pub. L. 102-88, title III, §§302-305(a), 306-307(b), Aug. 14, 1991, 105 Stat. 431-433; Pub. L. 102-183, title III, §§302(a)-(c), 303(a), 304-306(b), 307, 309(a), 310(a), Dec. 4, 1991, 105 Stat. 1262-1266; Pub. L. 102-496, title III, §304(b), Oct. 24, 1992, 106 Stat. 3183, known as the Central Intelligence Agency Retirement Act of 1964 for Certain Employees, was revised generally by Pub. L. 102-496, title VIII, §802, Oct. 24, 1992, 106 Stat. 3196. As so revised, Pub. L. 88-643, now known as the Central Intelligence Agency Retirement Act, has been transferred to chapter 38 (§2001 et seq.) of this title. All notes, Executive orders, and other provisions relating to this Act have been transferred to section 2001 of this title.

EXECUTIVE ORDER NO. 10656

Ex. Ord. No. 10656, Feb. 6, 1956, 21 F.R. 859, which established the President's Board of Consultants on Foreign Intelligence Activities, was revoked by Ex. Ord. No. 10938, May 4, 1961, 26 F.R. 3951, formerly set out below.

EXECUTIVE ORDER NO. 10938

Ex. Ord. No. 10938, May 4, 1961, 26 F.R. 3951, which established the President's Foreign Intelligence Advisory Board, was revoked by Ex. Ord. No. 11460, Mar. 20, 1969, 34 F.R. 5535, formerly set out below.

EXECUTIVE ORDER NO. 11460

Ex. Ord. No. 11460, Mar. 20, 1969, 34 F.R. 5535, which established the President's Foreign Intelligence Advisory Board, was revoked by Ex. Ord. No. 11984, May 4, 1977, 42 F.R. 23129, set out below.

EX. ORD. NO. 11984. ABOLITION OF PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD

Ex. Ord. No. 11984, May 4, 1977, 42 F.R. 23129, provided:

By virtue of the authority vested in me by the Constitution and statutes of the United States of America, and as President of the United States of America, in order to abolish the President's Foreign Intelligence Advisory Board, Executive Order No. 11460 of March 20, 1969, is hereby revoked.

JIMMY CARTER.

EXECUTIVE ORDER NO. 12331

Ex. Ord. No. 12331, Oct. 20, 1981, 46 F.R. 51705, which established the President's Foreign Intelligence Advisory Board, was revoked by Ex. Ord. No. 12537, Oct. 28, 1985, 50 F.R. 45083, formerly set out below.

EXECUTIVE ORDER NO. 12537

Ex. Ord. No. 12537, Oct. 28, 1985, 50 F.R. 45083, as amended by Ex. Ord. No. 12624, Jan. 6, 1988, 53 F.R. 489, which established the President's Foreign Intelligence Advisory Board, was revoked by Ex. Ord. No. 12863, §3.3, Sept. 13, 1993, 58 F.R. 48441, set out as a note under section 401 of this title.

§403-1. Responsibilities and authorities of the Director of National Intelligence

(a) Provision of intelligence

(1) The Director of National Intelligence shall be responsible for ensuring that national intelligence is provided—

(A) to the President;

(B) to the heads of departments and agencies of the executive branch;

(C) to the Chairman of the Joint Chiefs of Staff and senior military commanders;

(D) to the Senate and House of Representatives and the committees thereof; and

(E) to such other persons as the Director of National Intelligence determines to be appropriate.

(2) Such national intelligence should be timely, objective, independent of political considerations, and based upon all sources available to the intelligence community and other appropriate entities.

(b) Access to intelligence

Unless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any Federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence.

(c) Budget authorities

(1) With respect to budget requests and appropriations for the National Intelligence Program, the Director of National Intelligence shall—

(A) based on intelligence priorities set by the President, provide to the heads of departments containing agencies or organizations within the intelligence community, and to the heads of such agencies and organizations, guidance for developing the National Intelligence Program budget pertaining to such agencies and organizations;

(B) based on budget proposals provided to the Director of National Intelligence by the heads of agencies and organizations within the intelligence community and the heads of their respective departments and, as appropriate, after obtaining the advice of the Joint Intelligence Community Council, develop and determine an annual consolidated National Intelligence Program budget; and

(C) present such consolidated National Intelligence Program budget, together with any comments from the heads of departments containing agencies or organizations within the intelligence community, to the President for approval.

(2) In addition to the information provided under paragraph (1)(B), the heads of agencies and organizations within the intelligence community shall provide the Director of National Intelligence such other information as the Director shall request for the purpose of determining the annual consolidated National Intelligence Program budget under that paragraph.

(3)(A) The Director of National Intelligence shall participate in the development by the Secretary of Defense of the annual budgets for the Joint Military Intelligence Program and for Tactical Intelligence and Related Activities.

(B) The Director of National Intelligence shall provide guidance for the development of the annual budget for each element of the intelligence community that is not within the National Intelligence Program.

(4) The Director of National Intelligence shall ensure the effective execution of the annual budget for intelligence and intelligence-related activities.

(5)(A) The Director of National Intelligence shall be responsible for managing appropriations for the National Intelligence Program by directing the allotment or allocation of such appropriations through the heads of the departments containing agencies or organizations within the intelligence community and the Director of the Central Intelligence Agency, with prior notice (including the provision of appropriate supporting information) to the head of the department containing an agency or organization receiving any such allocation or allotment or the Director of the Central Intelligence Agency.

(B) Notwithstanding any other provision of law, pursuant to relevant appropriations Acts for the National Intelligence Program, the Director of the Office of Management and Budget shall exercise the authority of the Director of the Office of Management and Budget to apportion funds, at the exclusive direction of the Director of National Intelligence, for allocation to the elements of the intelligence community through the relevant host executive departments and the Central Intelligence Agency. Department comptrollers or appropriate budget execution officers shall allot, allocate, reprogram, or transfer funds appropriated for the National Intelligence Program in an expeditious manner.

(C) The Director of National Intelligence shall monitor the implementation and execution of the National Intelligence Program by the heads of the elements of the intelligence community that manage programs and activities that are part of the National Intelligence Program, which may include audits and evaluations.

(6) Apportionment and allotment of funds under this subsection shall be subject to chapter 13 and section 1517 of title 31 and the Congressional Budget and Impoundment Control Act of 1974 (2 U.S.C. 621 et seq.).

(7)(A) The Director of National Intelligence shall provide a semi-annual report, beginning April 1, 2005, and ending April 1, 2007, to the President and the Congress regarding implementation of this section.

(B) The Director of National Intelligence shall report to the President and the Congress not later than 15 days after learning of any instance in which a departmental comptroller acts in a manner inconsistent with the law (including permanent statutes, authorization Acts, and appropriations Acts), or the direction of the Director of National Intelligence, in carrying out the National Intelligence Program.

(d) Role of Director of National Intelligence in transfer and reprogramming of funds

(1)(A) No funds made available under the National Intelligence Program may be transferred or reprogrammed without the prior approval of the Director of National Intelligence, except in accordance with procedures prescribed by the Director of National Intelligence.

(B) The Secretary of Defense shall consult with the Director of National Intelligence before transferring or reprogramming funds made available under the Joint Military Intelligence Program.

(2) Subject to the succeeding provisions of this subsection, the Director of National Intelligence may transfer or reprogram funds appropriated for a program within the National Intelligence Program to another such program.

(3) The Director of National Intelligence may only transfer or reprogram funds referred to in subparagraph (A)—[1]

(A) with the approval of the Director of the Office of Management and Budget; and

(B) after consultation with the heads of departments containing agencies or organizations within the intelligence community to the extent such agencies or organizations are affected, and, in the case of the Central Intelligence Agency, after consultation with the Director of the Central Intelligence Agency.

(4) The amounts available for transfer or reprogramming in the National Intelligence Program in any given fiscal year, and the terms and conditions governing such transfers and reprogrammings, are subject to the provisions of annual appropriations Acts and this subsection.

(5)(A) A transfer or reprogramming of funds or personnel may be made under this subsection only if—

(i) the funds are being transferred to an activity that is a higher priority intelligence activity;

(ii) the transfer or reprogramming supports an emergent need, improves program effectiveness, or increases efficiency;

(iii) the transfer or reprogramming does not involve a transfer or reprogramming of funds to a Reserve for Contingencies of the Director of National Intelligence or the Reserve for Contingencies of the Central Intelligence Agency;

(iv) the transfer or reprogramming results in a cumulative transfer or reprogramming of funds out of any department or agency, as appropriate, funded in the National Intelligence Program in a single fiscal year—

(I) that is less than $150,000,000, and

(II) that is less than 5 percent of amounts available to a department or agency under the National Intelligence Program; and

(v) the transfer or reprogramming does not terminate an acquisition program.

[1] So in original. Probably should be "paragraph (1)(A)—".

(B) A transfer or reprogramming may be made without regard to a limitation set forth in clause (iv) or (v) of subparagraph (A) if the transfer has the concurrence of the head of the department involved or the Director of the Central Intelligence Agency (in the case of the Central Intelligence Agency). The authority to provide such concurrence may only be delegated by the head of the department or agency involved to the deputy of such officer.

(6) Funds transferred or reprogrammed under this subsection shall remain available for the same period as the appropriations account to which transferred or reprogrammed.

(7) Any transfer or reprogramming of funds under this subsection shall be carried out in accordance with existing procedures applicable to reprogramming notifications for the appropriate congressional committees. Any proposed transfer or reprogramming for which notice is given to the appropriate congressional committees shall be accompanied by a report explaining the nature of the proposed transfer or reprogramming and how it satisfies the requirements of this subsection. In addition, the congressional intelligence committees shall be promptly notified of any transfer or reprogramming of funds made pursuant to this subsection in any case in which the transfer or reprogramming would not have otherwise required reprogramming notification under procedures in effect as of December 17, 2004.

(e) Transfer of personnel

(1)(A) In addition to any other authorities available under law for such purposes, in the first twelve months after establishment of a new national intelligence center, the Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in consultation with the congressional committees of jurisdiction referred to in subparagraph (B), may transfer not more than 100 personnel authorized for elements of the intelligence community to such center.

(B) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

(ii) the Committees on Appropriations of the Senate and the House of Representatives;

(iii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

(iv) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(C) The Director shall include in any notice under subparagraph (B) an explanation of the nature of the transfer and how it satisfies the requirements of this subsection.

(2)(A) The Director of National Intelligence, with the approval of the Director of the Office of Management and Budget and in accordance with procedures to be developed by the Director of National Intelligence and the heads of the departments and agencies concerned, may transfer personnel authorized for an element of the intelligence community to another such element for a period of not more than 2 years.

(B) A transfer of personnel may be made under this paragraph only if—

(i) the personnel are being transferred to an activity that is a higher priority intelligence activity; and

(ii) the transfer supports an emergent need, improves program effectiveness, or increases efficiency.

(C) The Director of National Intelligence shall promptly provide notice of any transfer of personnel made pursuant to this paragraph to—

(i) the congressional intelligence committees;

(ii) in the case of the transfer of personnel to or from the Department of Defense, the Committees on Armed Services of the Senate and the House of Representatives; and

(iii) in the case of the transfer of personnel to or from the Department of Justice, to the Committees on the Judiciary of the Senate and the House of Representatives.

(D) The Director shall include in any notice under subparagraph (C) an explanation of the nature of the transfer and how it satisfies the requirements of this paragraph.

(3) It is the sense of Congress that—

(A) the nature of the national security threats facing the United States will continue to challenge the intelligence community to respond rapidly and flexibly to bring analytic resources to bear against emerging and unforeseen requirements;

(B) both the Office of the Director of National Intelligence and any analytic centers determined to be necessary should be fully and properly supported with appropriate levels of personnel resources and that the President's yearly budget requests adequately support those needs; and

(C) the President should utilize all legal and administrative discretion to ensure that the Director of National Intelligence and all other elements of the intelligence community have the necessary resources and procedures to respond promptly and effectively to emerging and unforeseen national security challenges.

(f) Tasking and other authorities

(1)(A) The Director of National Intelligence shall—

(i) establish objectives, priorities, and guidance for the intelligence community to ensure timely and effective collection, processing, analysis, and dissemination (including access by users to collected data consistent with applicable law and, as appropriate, the guidelines referred to in subsection (b) of this section and analytic products generated by or within the intelligence community) of national intelligence;

(ii) determine requirements and priorities for, and manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community, including—

(I) approving requirements (including those requirements responding to needs provided by consumers) for collection and analysis; and

(II) resolving conflicts in collection requirements and in the tasking of national collection assets of the elements of the intelligence community; and

(iii) provide advisory tasking to intelligence elements of those agencies and departments not within the National Intelligence Program.

(B) The authority of the Director of National Intelligence under subparagraph (A) shall not apply—

(i) insofar as the President so directs;

(ii) with respect to clause (ii) of subparagraph (A), insofar as the Secretary of Defense exercises tasking authority under plans or arrangements agreed upon by the Secretary of Defense and the Director of National Intelligence; or

(iii) to the direct dissemination of information to State government and local government officials and private sector entities pursuant to sections 121 and 482 of title 6.

(2) The Director of National Intelligence shall oversee the National Counterterrorism Center and may establish such other national intelligence centers as the Director determines necessary.

(3)(A) The Director of National Intelligence shall prescribe, in consultation with the heads of other agencies or elements of the intelligence community, and the heads of their respective departments, personnel policies and programs applicable to the intelligence community that—

(i) encourage and facilitate assignments and details of personnel to national intelligence centers, and between elements of the intelligence community;

(ii) set standards for education, training, and career development of personnel of the intelligence community;

(iii) encourage and facilitate the recruitment and retention by the intelligence community of highly qualified individuals for the effective conduct of intelligence activities;

(iv) ensure that the personnel of the intelligence community are sufficiently diverse for purposes of the collection and analysis of intelligence through the recruitment and training of women, minorities, and individuals with diverse ethnic, cultural, and linguistic backgrounds;

(v) make service in more than one element of the intelligence community a condition of promotion to such positions within the intelligence community as the Director shall specify; and

(vi) ensure the effective management of intelligence community personnel who are responsible for intelligence community-wide matters.

(B) Policies prescribed under subparagraph (A) shall not be inconsistent with the personnel policies otherwise applicable to members of the uniformed services.

(4) The Director of National Intelligence shall ensure compliance with the Constitution and laws of the United States by the Central Intelligence Agency and shall ensure such compliance by other elements of the intelligence community through the host executive departments that manage the programs and activities that are part of the National Intelligence Program.

(5) The Director of National Intelligence shall ensure the elimination of waste and unnecessary duplication within the intelligence community.

(6) The Director of National Intelligence shall establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for national intelligence purposes, except that the Director shall have no authority to direct or undertake electronic surveillance or physical search operations pursuant to that Act unless authorized by statute or Executive order.

(7) The Director of National Intelligence shall perform such other functions as the President may direct.

(8) Nothing in this subchapter shall be construed as affecting the role of the Department of Justice or the Attorney General under the Foreign Intelligence Surveillance Act of 1978.

(g) Intelligence information sharing

(1) The Director of National Intelligence shall have principal authority to ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements. The Director of National Intelligence shall—

(A) establish uniform security standards and procedures;

(B) establish common information technology standards, protocols, and interfaces;

(C) ensure development of information technology systems that include multi-level security and intelligence integration capabilities;

(D) establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods;

(E) develop an enterprise architecture for the intelligence community and ensure that elements of the intelligence community comply with such architecture; and

(F) have procurement approval authority over all enterprise architecture-related information technology items funded in the National Intelligence Program.

(2) The President shall ensure that the Director of National Intelligence has all necessary support and authorities to fully and effectively implement paragraph (1).

(3) Except as otherwise directed by the President or with the specific written agreement of the head of the department or agency in question, a Federal agency or official shall not be considered to have met any obligation to provide any information, report, assessment, or other material (including unevaluated intelligence information) to that department or agency solely by virtue of having provided that information, report, assessment, or other material to the Director of National Intelligence or the National Counterterrorism Center.

(4) Not later than February 1 of each year, the Director of National Intelligence shall submit to

the President and to the Congress an annual report that identifies any statute, regulation, policy, or practice that the Director believes impedes the ability of the Director to fully and effectively implement paragraph (1).

(h) Analysis

To ensure the most accurate analysis of intelligence is derived from all sources to support national security needs, the Director of National Intelligence shall—

(1) implement policies and procedures—

(A) to encourage sound analytic methods and tradecraft throughout the elements of the intelligence community;

(B) to ensure that analysis is based upon all sources available; and

(C) to ensure that the elements of the intelligence community regularly conduct competitive analysis of analytic products, whether such products are produced by or disseminated to such elements;

(2) ensure that resource allocation for intelligence analysis is appropriately proportional to resource allocation for intelligence collection systems and operations in order to maximize analysis of all collected data;

(3) ensure that differences in analytic judgment are fully considered and brought to the attention of policymakers; and

(4) ensure that sufficient relationships are established between intelligence collectors and analysts to facilitate greater understanding of the needs of analysts.

(i) Protection of intelligence sources and methods

(1) The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.

(2) Consistent with paragraph (1), in order to maximize the dissemination of intelligence, the Director of National Intelligence shall establish and implement guidelines for the intelligence community for the following purposes:

(A) Classification of information under applicable law, Executive orders, or other Presidential directives.

(B) Access to and dissemination of intelligence, both in final form and in the form when initially gathered.

(C) Preparation of intelligence products in such a way that source information is removed to allow for dissemination at the lowest level of classification possible or in unclassified form to the extent practicable.

(3) The Director may only delegate a duty or authority given the Director under this subsection to the Principal Deputy Director of National Intelligence.

(j) Uniform procedures for sensitive compartmented information

The Director of National Intelligence, subject to the direction of the President, shall—

(1) establish uniform standards and procedures for the grant of access to sensitive compartmented information to any officer or employee of any agency or department of the United States and to employees of contractors of those agencies or departments;

(2) ensure the consistent implementation of those standards and procedures throughout such agencies and departments;

(3) ensure that security clearances granted by individual elements of the intelligence community are recognized by all elements of the intelligence community, and under contracts entered into by those agencies; and

(4) ensure that the process for investigation and adjudication of an application for access to sensitive compartmented information is performed in the most expeditious manner possible consistent with applicable standards for national security.

(k) Coordination with foreign governments

Under the direction of the President and in a manner consistent with section 3927 of title 22, the Director of National Intelligence shall oversee the coordination of the relationships between elements of the intelligence community and the intelligence or security services of foreign governments or international organizations on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means.

***(l)* Enhanced personnel management**

(1)(A) The Director of National Intelligence shall, under regulations prescribed by the Director, provide incentives for personnel of elements of the intelligence community to serve—

(i) on the staff of the Director of National Intelligence;

(ii) on the staff of the national intelligence centers;

(iii) on the staff of the National Counterterrorism Center; and

(iv) in other positions in support of the intelligence community management functions of the Director.

(B) Incentives under subparagraph (A) may include financial incentives, bonuses, and such other awards and incentives as the Director considers appropriate.

(2)(A) Notwithstanding any other provision of law, the personnel of an element of the intelligence community who are assigned or detailed under paragraph (1)(A) to service under the Director of National Intelligence shall be promoted at rates equivalent to or better than personnel of such element who are not so assigned or detailed.

(B) The Director may prescribe regulations to carry out this section.

(3)(A) The Director of National Intelligence shall prescribe mechanisms to facilitate the rotation of personnel of the intelligence community through various elements of the intelligence community in the course of their careers in order to facilitate the widest possible understanding by such personnel of the variety of intelligence requirements, methods, users, and capabilities.

(B) The mechanisms prescribed under subparagraph (A) may include the following:

(i) The establishment of special occupational categories involving service, over the course of a career, in more than one element of the intelligence community.

(ii) The provision of rewards for service in positions undertaking analysis and planning

of operations involving two or more elements of the intelligence community.

(iii) The establishment of requirements for education, training, service, and evaluation for service involving more than one element of the intelligence community.

(C) It is the sense of Congress that the mechanisms prescribed under this subsection should, to the extent practical, seek to duplicate for civilian personnel within the intelligence community the joint officer management policies established by chapter 38 of title 10 and the other amendments made by title IV of the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Public Law 99-433).

(4)(A) Except as provided in subparagraph (B) and subparagraph (D), this subsection shall not apply with respect to personnel of the elements of the intelligence community who are members of the uniformed services.

(B) Mechanisms that establish requirements for education and training pursuant to paragraph (3)(B)(iii) may apply with respect to members of the uniformed services who are assigned to an element of the intelligence community funded through the National Intelligence Program, but such mechanisms shall not be inconsistent with personnel policies and education and training requirements otherwise applicable to members of the uniformed services.

(C) The personnel policies and programs developed and implemented under this subsection with respect to law enforcement officers (as that term is defined in section 5541(3) of title 5) shall not affect the ability of law enforcement entities to conduct operations or, through the applicable chain of command, to control the activities of such law enforcement officers.

(D) Assignment to the Office of the Director of National Intelligence of commissioned officers of the Armed Forces shall be considered a joint-duty assignment for purposes of the joint officer management policies prescribed by chapter 38 of title 10 and other provisions of that title.

(m) Additional authority with respect to personnel

(1) In addition to the authorities under subsection (f)(3) of this section, the Director of National Intelligence may exercise with respect to the personnel of the Office of the Director of National Intelligence any authority of the Director of the Central Intelligence Agency with respect to the personnel of the Central Intelligence Agency under the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.), and other applicable provisions of law, as of December 17, 2004, to the same extent, and subject to the same conditions and limitations, that the Director of the Central Intelligence Agency may exercise such authority with respect to personnel of the Central Intelligence Agency.

(2) Employees and applicants for employment of the Office of the Director of National Intelligence shall have the same rights and protections under the Office of the Director of National Intelligence as employees of the Central Intelligence Agency have under the Central Intelligence Agency Act of 1949 [50 U.S.C. 403a et seq.], and other applicable provisions of law, as of December 17, 2004.

(n) Acquisition authorities

(1) In carrying out the responsibilities and authorities under this section, the Director of National Intelligence may exercise the acquisition and appropriations authorities referred to in the Central Intelligence Agency Act of 1949 (50 U.S.C. 403a et seq.) other than the authorities referred to in section 8(b) of that Act (50 U.S.C. 403j(b)).

(2) For the purpose of the exercise of any authority referred to in paragraph (1), a reference to the head of an agency shall be deemed to be a reference to the Director of National Intelligence or the Principal Deputy Director of National Intelligence.

(3)(A) Any determination or decision to be made under an authority referred to in paragraph (1) by the head of an agency may be made with respect to individual purchases and contracts or with respect to classes of purchases or contracts, and shall be final.

(B) Except as provided in subparagraph (C), the Director of National Intelligence or the Principal Deputy Director of National Intelligence may, in such official's discretion, delegate to any officer or other official of the Office of the Director of National Intelligence any authority to make a determination or decision as the head of the agency under an authority referred to in paragraph (1).

(C) The limitations and conditions set forth in section 3(d) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403c(d)) shall apply to the exercise by the Director of National Intelligence of an authority referred to in paragraph (1).

(D) Each determination or decision required by an authority referred to in the second sentence of section 3(d) of the Central Intelligence Agency Act of 1949 [50 U.S.C. 403c(d)] shall be based upon written findings made by the official making such determination or decision, which findings shall be final and shall be available within the Office of the Director of National Intelligence for a period of at least six years following the date of such determination or decision.

(o) Consideration of views of elements of intelligence community

In carrying out the duties and responsibilities under this section, the Director of National Intelligence shall take into account the views of a head of a department containing an element of the intelligence community and of the Director of the Central Intelligence Agency.

(p) Responsibility of Director of National Intelligence regarding National Intelligence Program budget concerning the Department of Defense

Subject to the direction of the President, the Director of National Intelligence shall, after consultation with the Secretary of Defense, ensure that the National Intelligence Program budgets for the elements of the intelligence community that are within the Department of Defense are adequate to satisfy the national intelligence needs of the Department of Defense, including the needs of the Chairman of the Joint Chiefs of Staff and the commanders of the unified and specified commands, and wherever such

elements are performing Government-wide functions, the needs of other Federal departments and agencies.

(q) Acquisitions of major systems

(1) For each intelligence program within the National Intelligence Program for the acquisition of a major system, the Director of National Intelligence shall—

(A) require the development and implementation of a program management plan that includes cost, schedule, and performance goals and program milestone criteria, except that with respect to Department of Defense programs the Director shall consult with the Secretary of Defense;

(B) serve as exclusive milestone decision authority, except that with respect to Department of Defense programs the Director shall serve as milestone decision authority jointly with the Secretary of Defense or the designee of the Secretary; and

(C) periodically—

(i) review and assess the progress made toward the achievement of the goals and milestones established in such plan; and

(ii) submit to Congress a report on the results of such review and assessment.

(2) If the Director of National Intelligence and the Secretary of Defense are unable to reach an agreement on a milestone decision under paragraph (1)(B), the President shall resolve the conflict.

(3) Nothing in this subsection may be construed to limit the authority of the Director of National Intelligence to delegate to any other official any authority to perform the responsibilities of the Director under this subsection.

(4) In this subsection:

(A) The term "intelligence program", with respect to the acquisition of a major system, means a program that—

(i) is carried out to acquire such major system for an element of the intelligence community; and

(ii) is funded in whole out of amounts available for the National Intelligence Program.

(B) The term "major system" has the meaning given such term in section 403(9) of title 41.

(r) Performance of common services

The Director of National Intelligence shall, in consultation with the heads of departments and agencies of the United States Government containing elements within the intelligence community and with the Director of the Central Intelligence Agency, coordinate the performance by the elements of the intelligence community within the National Intelligence Program of such services as are of common concern to the intelligence community, which services the Director of National Intelligence determines can be more efficiently accomplished in a consolidated manner.

(July 26, 1947, ch. 343, title I, § 102A, as added Pub. L. 108–458, title I, § 1011(a), Dec. 17, 2004, 118 Stat. 3644.)

REFERENCES IN TEXT

The Congressional Budget and Impoundment Control Act of 1974, referred to in subsec. (c)(6), is Pub. L. 93–344, July 12, 1974, 88 Stat. 297, as amended. For complete classification of this Act to the Code, see Short Title note set out under section 621 of Title 2, The Congress, and Tables.

The Foreign Intelligence Surveillance Act of 1978, referred to in subsec. (f)(6), (8), is Pub. L. 95–511, Oct. 25, 1978, 92 Stat. 1783, as amended, which is classified principally to chapter 36 (§ 1801 et seq.) of this title. For complete classification of this Act to the Code, see Short Title note set out under section 1801 of this title and Tables.

This subchapter, referred to in subsec. (f)(8), was in the original "this title", meaning title I of act July 26, 1947, ch. 343, 61 Stat. 496, as amended, which is classified generally to this subchapter. For complete classification of title I to the Code, see Tables.

The Goldwater-Nichols Department of Defense Reorganization Act of 1986, referred to in subsec. (f)(3)(C), is Pub. L. 99–433, Oct. 1, 1986, 100 Stat. 992, as amended. For complete classification of this Act to the Code, see Short Title of 1986 Amendment note set out under section 111 of Title 10, Armed Forces, and Tables.

The Central Intelligence Agency Act of 1949, referred to in subsecs. (m) and (n)(1), is act June 20, 1949, ch. 227, 63 Stat. 208, as amended, which is classified generally to section 403a et seq. of this title. For complete classification of this Act to the Code, see Short Title note set out under section 403a of this title and Tables.

PRIOR PROVISIONS

A prior section 403–1, act July 26, 1947, ch. 343, title I, § 102A, as added Pub. L. 104–293, title VIII, § 805(b), Oct. 11, 1996, 110 Stat. 3479, provided there is a Central Intelligence Agency and described its function prior to repeal by Pub. L. 108–458, title I, §§ 1011(a), 1097(a), Dec. 17, 2004, 118 Stat. 3643, 3698, effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided. See section 403–4 of this title.

Another prior section 403–1, act July 26, 1947, ch. 343, title I, § 102a, as added Dec. 9, 1983, Pub. L. 98–215, title IV, § 403, 97 Stat. 1477, related to appointment of Director of the Intelligence Community Staff prior to repeal by Pub. L. 102–496, title VII, § 705(a)(1), Oct. 24, 1992, 106 Stat. 3190.

EFFECTIVE DATE

For Determination by President that section take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 401 of this title.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108–458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 401 of this title.

JOINT PROCEDURES FOR OPERATIONAL COORDINATION BETWEEN DEPARTMENT OF DEFENSE AND CENTRAL INTELLIGENCE AGENCY

Pub. L. 108–458, title I, § 1013, Dec. 17, 2004, 118 Stat. 3662, provided that:

"(a) DEVELOPMENT OF PROCEDURES.—The Director of National Intelligence, in consultation with the Secretary of Defense and the Director of the Central Intelligence Agency, shall develop joint procedures to be used by the Department of Defense and the Central Intelligence Agency to improve the coordination and deconfliction of operations that involve elements of both the Armed Forces and the Central Intelligence Agency consistent with national security and the protection of human intelligence sources and methods. Those procedures shall, at a minimum, provide the following:

"(1) Methods by which the Director of the Central Intelligence Agency and the Secretary of Defense can improve communication and coordination in the planning, execution, and sustainment of operations, including, as a minimum—

"(A) information exchange between senior officials of the Central Intelligence Agency and senior

officers and officials of the Department of Defense when planning for such an operation commences by either organization; and

"(B) exchange of information between the Secretary and the Director of the Central Intelligence Agency to ensure that senior operational officials in both the Department of Defense and the Central Intelligence Agency have knowledge of the existence of the ongoing operations of the other.

"(2) When appropriate, in cases where the Department of Defense and the Central Intelligence Agency are conducting separate missions in the same geographical area, a mutual agreement on the tactical and strategic objectives for the region and a clear delineation of operational responsibilities to prevent conflict and duplication of effort.

"(b) IMPLEMENTATION REPORT.—Not later than 180 days after the date of the enactment of the Act [Dec. 17, 2004], the Director of National Intelligence shall submit to the congressional defense committees (as defined in section 101 of title 10, United States Code) and the congressional intelligence committees (as defined in section 3(7) of the National Security Act of 1947 (50 U.S.C. 401a(7))) a report describing the procedures established pursuant to subsection (a) and the status of the implementation of those procedures."

ALTERNATIVE ANALYSIS OF INTELLIGENCE BY THE INTELLIGENCE COMMUNITY

Pub. L. 108-458, title I, §1017, Dec. 17, 2004, 118 Stat. 3670, provided that:

"(a) IN GENERAL.—Not later than 180 days after the effective date of this Act [probably means the effective date of title I of Pub. L. 108-458, see Effective Date of 2004 Amendment; Transition Provisions note set out under section 401 of this title], the Director of National Intelligence shall establish a process and assign an individual or entity the responsibility for ensuring that, as appropriate, elements of the intelligence community conduct alternative analysis (commonly referred to as 'red-team analysis') of the information and conclusions in intelligence products.

"(b) REPORT.—Not later than 270 days after the effective date of this Act, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee of the House of Representatives on the implementation of subsection (a)."

REQUIREMENT FOR EFFICIENT USE BY INTELLIGENCE COMMUNITY OF OPEN-SOURCE INTELLIGENCE

Pub. L. 108-458, title I, §1052(b), Dec. 17, 2004, 118 Stat. 3683, provided that: "The Director of National Intelligence shall ensure that the intelligence community makes efficient and effective use of open-source information and analysis."

ENHANCING CLASSIFIED COUNTERTERRORIST TRAVEL EFFORTS

Pub. L. 108-458, title VII, §7201(e), Dec. 17, 2004, 118 Stat. 3813, provided that:

"(1) IN GENERAL.—The Director of National Intelligence shall significantly increase resources and personnel to the small classified program that collects and analyzes intelligence on terrorist travel.

"(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for each of the fiscal years 2005 through 2009 such sums as may be necessary to carry out this subsection."

INTELLIGENCE COMMUNITY USE OF NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER

Pub. L. 108-458, title VIII, §8101, Dec. 17, 2004, 118 Stat. 3864, provided that:

"(a) IN GENERAL.—The Director of National Intelligence shall establish a formal relationship, including information sharing, between the elements of the intelligence community and the National Infrastructure Simulation and Analysis Center.

"(b) PURPOSE.—The purpose of the relationship under subsection (a) shall be to permit the intelligence community to take full advantage of the capabilities of the National Infrastructure Simulation and Analysis Center, particularly vulnerability and consequence analysis, for real time response to reported threats and long term planning for projected threats."

PILOT PROGRAM ON ANALYSIS OF SIGNALS AND OTHER INTELLIGENCE BY INTELLIGENCE ANALYSTS OF VARIOUS ELEMENTS OF THE INTELLIGENCE COMMUNITY

Pub. L. 108-177, title III, §317, Dec. 13, 2003, 117 Stat. 2511, as amended by Pub. L. 108-458, title I, §§1071(g)(3)(A)(i), (ii), 1072(d)(2)(A), Dec. 17, 2004, 118 Stat. 3692, 3693, provided that:

"(a) IN GENERAL.—The Director of National Intelligence shall, in coordination with the Secretary of Defense, carry out a pilot program to assess the feasibility and advisability of permitting intelligence analysts of various elements of the intelligence community to access and analyze intelligence from the databases of other elements of the intelligence community in order to achieve the objectives set forth in subsection (c).

"(b) COVERED INTELLIGENCE.—The intelligence to be analyzed under the pilot program under subsection (a) shall include the following:

"(1) Signals intelligence of the National Security Agency.

"(2) Such intelligence of other elements of the intelligence community as the Director shall select for purposes of the pilot program.

"(c) OBJECTIVES.—The objectives set forth in this subsection are as follows:

"(1) To enhance the capacity of the intelligence community to undertake 'all source fusion' analysis in support of the intelligence and intelligence-related missions of the intelligence community.

"(2) To reduce, to the extent possible, the amount of intelligence collected by the intelligence community that is not assessed, or reviewed, by intelligence analysts.

"(3) To reduce the burdens imposed on analytical personnel of the elements of the intelligence community by current practices regarding the sharing of intelligence among elements of the intelligence community.

"(d) COMMENCEMENT.—The Director shall commence the pilot program under subsection (a) not later than December 31, 2003.

"(e) VARIOUS MECHANISMS REQUIRED.—In carrying out the pilot program under subsection (a), the Director shall develop and utilize various mechanisms to facilitate the access to, and the analysis of, intelligence in the databases of the intelligence community by intelligence analysts of other elements of the intelligence community, including the use of so-called 'detailees in place'.

"(f) SECURITY.—(1) In carrying out the pilot program under subsection (a), the Director shall take appropriate actions to protect against the disclosure and unauthorized use of intelligence in the databases of the elements of the intelligence community which may endanger sources and methods which (as determined by the Director) warrant protection.

"(2) The actions taken under paragraph (1) shall include the provision of training on the accessing and handling of information in the databases of various elements of the intelligence community and the establishment of limitations on access to information in such databases regarding United States persons.

"(g) ASSESSMENT.—Not later than February 1, 2004, after the commencement under subsection (d) of the pilot program under subsection (a), the Under Secretary of Defense for Intelligence and the Deputy Director of National Intelligence shall jointly carry out an assessment of the progress of the pilot program in meeting the objectives set forth in subsection (c).

"(h) REPORT.—(1) The Director of National Intelligence shall, in coordination with the Secretary of Defense, submit to the appropriate committees of Con-

gress a report on the assessment carried out under subsection (g).

"(2) The report shall include—

"(A) a description of the pilot program under subsection (a);

"(B) the findings of the Under Secretary and Assistant Director [Deputy Director of National Intelligence] as a result of the assessment;

"(C) any recommendations regarding the pilot program that the Under Secretary and the Deputy Director of National Intelligence jointly consider appropriate in light of the assessment; and

"(D) any recommendations that the Director and Secretary consider appropriate for purposes of the report.

"(i) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term 'appropriate committees of Congress' means—

"(1) the Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Appropriations of the Senate; and

"(2) the Permanent Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Appropriations of the House of Representatives."

STANDARDIZED TRANSLITERATION OF NAMES INTO THE ROMAN ALPHABET

Pub. L. 107-306, title III, §352, Nov. 27, 2002, 116 Stat. 2401, as amended by Pub. L. 108-458, title I, §1071(g)(2)(D), Dec. 17, 2004, 118 Stat. 3691, provided that:

"(a) METHOD OF TRANSLITERATION REQUIRED.—Not later than 180 days after the date of the enactment of this Act [Nov. 27, 2002], the Director of Central Intelligence shall provide for a standardized method for transliterating into the Roman alphabet personal and place names originally rendered in any language that uses an alphabet other than the Roman alphabet.

"(b) USE BY INTELLIGENCE COMMUNITY.—The Director of National Intelligence shall ensure the use of the method established under subsection (a) in—

"(1) all communications among the elements of the intelligence community; and

"(2) all intelligence products of the intelligence community."

STANDARDS FOR SPELLING OF FOREIGN NAMES AND PLACES AND FOR USE OF GEOGRAPHIC COORDINATES

Pub. L. 105-107, title III, §309, Nov. 20, 1997, 111 Stat. 2253, provided that:

"(a) SURVEY OF CURRENT STANDARDS.—

"(1) SURVEY.—The Director of Central Intelligence shall carry out a survey of current standards for the spelling of foreign names and places, and the use of geographic coordinates for such places, among the elements of the intelligence community.

"(2) REPORT.—Not later than 90 days after the date of enactment of this Act [Nov. 20, 1997], the Director shall submit to the congressional intelligence committees a report on the survey carried out under paragraph (1). The report shall be submitted in unclassified form, but may include a classified annex.

"(b) GUIDELINES.—

"(1) ISSUANCE.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidelines to ensure the use of uniform spelling of foreign names and places and the uniform use of geographic coordinates for such places. The guidelines shall apply to all intelligence reports, intelligence products, and intelligence databases prepared and utilized by the elements of the intelligence community.

"(2) BASIS.—The guidelines under paragraph (1) shall, to the maximum extent practicable, be based on current United States Government standards for the transliteration of foreign names, standards for foreign place names developed by the Board on Geographic Names, and a standard set of geographic coordinates.

"(3) SUBMITTAL TO CONGRESS.—The Director shall submit a copy of the guidelines to the congressional intelligence committees.

"(c) CONGRESSIONAL INTELLIGENCE COMMITTEES DEFINED.—In this section, the term 'congressional intelligence committees' means the following:

"(1) The Select Committee on Intelligence of the Senate.

"(2) The Permanent Select Committee on Intelligence of the House of Representatives."

[Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 401 of this title.]

PERIODIC REPORTS ON EXPENDITURES

Pub. L. 104-293, §807(c), Oct. 11, 1996, 110 Stat. 3480, provided that: "Not later than January 1, 1997, the Director of Central Intelligence and the Secretary of Defense shall prescribe guidelines to ensure prompt reporting to the Director and the Secretary on a periodic basis of budget execution data for all national, defense-wide, and tactical intelligence activities."

[Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 401 of this title.]

DATABASE PROGRAM TRACKING

Pub. L. 104-293, title VIII, §807(d), Oct. 11, 1996, 110 Stat. 3481, provided that: "Not later than January 1, 1999, the Director of Central Intelligence and the Secretary of Defense shall develop and implement a database to provide timely and accurate information on the amounts, purposes, and status of the resources, including periodic budget execution updates, for all national, defense-wide, and tactical intelligence activities."

[Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108-458, set out as a note under section 401 of this title.]

IDENTIFICATION OF CONSTITUENT COMPONENTS OF BASE INTELLIGENCE BUDGET

Pub. L. 103-359, title VI, §603, Oct. 14, 1994, 108 Stat. 3433, provided that: "The Director of Central Intelligence shall include the same level of budgetary detail for the Base Budget that is provided for Ongoing Initiatives and New Initiatives to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate in the congressional justification materials for the annual submission of the National Foreign Intelligence Program of each fiscal year."

[Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of Na-

tional Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 401 of this title.]

§403–1a. Assignment of responsibilities relating to analytic integrity

(a) Assignment of responsibilities

For purposes of carrying out section 403–1(h) of this title, the Director of National Intelligence shall, not later than 180 days after December 17, 2004, assign an individual or entity to be responsible for ensuring that finished intelligence products produced by any element or elements of the intelligence community are timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic tradecraft.

(b) Responsibilities

(1) The individual or entity assigned responsibility under subsection (a) of this section—

(A) may be responsible for general oversight and management of analysis and production, but may not be directly responsible for, or involved in, the specific production of any finished intelligence product;

(B) shall perform, on a regular basis, detailed reviews of finished intelligence product or other analytic products by an element or elements of the intelligence community covering a particular topic or subject matter;

(C) shall be responsible for identifying on an annual basis functional or topical areas of analysis for specific review under subparagraph (B); and

(D) upon completion of any review under subparagraph (B), may draft lessons learned, identify best practices, or make recommendations for improvement to the analytic tradecraft employed in the production of the reviewed product or products.

(2) Each review under paragraph (1)(B) should—

(A) include whether the product or products concerned were based on all sources of available intelligence, properly describe the quality and reliability of underlying sources, properly caveat and express uncertainties or confidence in analytic judgments, properly distinguish between underlying intelligence and the assumptions and judgments of analysts, and incorporate, where appropriate, alternative analyses; and

(B) ensure that the analytic methodologies, tradecraft, and practices used by the element or elements concerned in the production of the product or products concerned meet the standards set forth in subsection (a) of this section.

(3) Information drafted under paragraph (1)(D) should, as appropriate, be included in analysis teaching modules and case studies for use throughout the intelligence community.

(c) Annual reports

Not later than December 1 each year, the Director of National Intelligence shall submit to the congressional intelligence committees, the heads of the relevant elements of the intelligence community, and the heads of analytic training departments a report containing a description, and the associated findings, of each review under subsection (b)(1)(B) of this section during such year.

(d) Congressional intelligence committees defined

In this section, the term "congressional intelligence committees" means—

(1) the Select Committee on Intelligence of the Senate; and

(2) the Permanent Select Committee on Intelligence of the House of Representatives.

(Pub. L. 108–458, title I, §1019, Dec. 17, 2004, 118 Stat. 3671.)

CODIFICATION

Section was enacted as part of the Intelligence Reform and Terrorism Prevention Act of 2004, and also as part of the National Security Intelligence Reform Act of 2004, and not as part of the National Security Act of 1947 which comprises this chapter.

EFFECTIVE DATE

For Determination by President that section take effect on Apr. 21, 2005, see Memorandum of President of the United States, Apr. 21, 2005, 70 F.R. 23925, set out as a note under section 401 of this title.

Section effective not later than six months after Dec. 17, 2004, except as otherwise expressly provided, see section 1097(a) of Pub. L. 108–458, set out in an Effective Date of 2004 Amendment; Transition Provisions note under section 401 of this title.

SAFEGUARD OF OBJECTIVITY IN INTELLIGENCE ANALYSIS

Pub. L. 108–458, title I, §1020, Dec. 17, 2004, 118 Stat. 3672, provided that:

"(a) IN GENERAL.—Not later than 180 days after the effective date of this Act [probably means the effective date of title I of Pub. L. 108–458, see Effective Date of 2004 Amendment; Transition Provisions note set out under section 401 of this title], the Director of National Intelligence shall identify an individual within the Office of the Director of National Intelligence who shall be available to analysts within the Office of the Director of National Intelligence to counsel, conduct arbitration, offer recommendations, and, as appropriate, initiate inquiries into real or perceived problems of analytic tradecraft or politicization, biased reporting, or lack of objectivity in intelligence analysis.

"(b) REPORT.—Not later than 270 days after the effective date of this Act, the Director of National Intelligence shall provide a report to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives on the implementation of subsection (a)."

§403–1b. Additional education and training requirements

(a) Findings

Congress makes the following findings:

(1) Foreign language education is essential for the development of a highly-skilled workforce for the intelligence community.

(2) Since September 11, 2001, the need for language proficiency levels to meet required national security functions has been raised, and the ability to comprehend and articulate technical and scientific information in foreign languages has become critical.

(b) Linguistic requirements

(1) The Director of National Intelligence shall—

ANNEX 4

Executive Order 12333, as amended

56838.200

UNITED STATES INTELLIGENCE ACTIVITIES
DECEMBER 4, 1981
(AS AMENDED BY EXECUTIVE ORDERS 13284 (2003), 13355 (2004) AND 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 *Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts*

1.1 *Goals.* The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of

56838.201

and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

(1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;

(2) Threats to the United States and its interests from terrorism; and

(3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into

56838.202

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 *The National Security Council.*

(a) *Purpose.* The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) *Covert Action and Other Sensitive Intelligence Operations.* The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 *Director of National Intelligence.* Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and

56838.203

shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and

56838.204

heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems,

56838.205

assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

56838.206

declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for

56838.207

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements,

56838.208

elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish

procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence

56838.209

human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

56838.210

activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence

56838.211

Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense

56838.212

the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

56838.213

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with

56838.214

information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 *Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies.* The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not

56838.215

(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or

56838.216

consultation with the Director of National Intelligence.

1.6 *Heads of Elements of the Intelligence Community.* The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State,

56838.217

accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 *Intelligence Community Elements.* Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

56838.218

President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the

56838.219

activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and

56838.220

activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating

56838.221

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with

56838.222

INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison

56838.223

1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center,

56838.224

shall:

(a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 *The Department of the Treasury.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 *The Department of Defense.* The Secretary of Defense shall:

(a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;

(b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution

56838.225

of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform

56838.226

Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense,

(h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 *The Department of Homeland Security.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 *The Department of Energy.* In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and

56838.227

Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 *The Federal Bureau of Investigation.* In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2 *Conduct of Intelligence Activities*

2.1 *Need.* Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 *Purpose.* This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence,

56838.228

with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 *Collection of information.* Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States

56838.229

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be

56838.230

2.4 *Collection Techniques.* Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

56838.231

than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 *Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 *Assistance to Law Enforcement and other Civil Authorities.* Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property,

56838.232

or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 *Contracting*. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 *Consistency With Other Laws*. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 *Undisclosed Participation in Organizations Within the United States*. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established

56838.233

to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 *Human Experimentation.* No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 *Prohibition on Assassination.* No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 *Indirect Participation.* No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 *Limitation on Covert Action.* No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 *General Provisions*

3.1 *Congressional Oversight.* The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to

56838.234

including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 *Implementation.* The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 *Procedures.* The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

56838.235

President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 *Definitions.* For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

56838.236

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community* and elements of the Intelligence Community refers to:

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

56838.237

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this

56838.238

bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 *Revocation.* Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 *General Provisions.*

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

(1) Authority granted by law to a department or agency, or the head thereof; or

(2) Functions of the Director of the Office of

56838.239

appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

/s/ Ronald Reagan

THE WHITE HOUSE

December 4, 1981

56838.240

Testimony Of Jeffrey H. Smith[1]
Senate Committee on Homeland Security and Governmental Affairs
March 17, 2010

Mr. Chairman, thank you for inviting me to appear this morning to discuss a very important topic, namely the implementation of the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA") that established the Director of National Intelligence ("DNI") some five years ago. In particular, you have asked me to reflect on the role of the DNI and the organization of the Intelligence Community in light of the failure to prevent Abdul Farouk Abdulmutallab, the "Christmas bomber," from getting on an airplane bound for the United States with a concealed bomb.

I am very pleased that the Committee is taking a hard look at how the statute has worked. And I must be candid: It is not working as well as it should.

To prepare for these hearings, I spoke to many senior Intelligence Community officers, including in the Office of the Director of National Intelligence ("ODNI"). My testimony this morning draws on those conversations and my own experiences over the years. What I found was very disturbing. It leads me to conclude that there is an urgent need for a serious in-depth look at the organization and functioning of the American Intelligence Community.

The Intelligence Community is very large and complex. It is a unique beast in the American government - sixteen agencies spread throughout seven separate government

[1] It has been my privilege to work in and with the U.S. Intelligence Community for 35 years, since I was hired in 1975 by the Office of the Legal Adviser of the Department of State to be the junior lawyer helping the department with the Church and Pike Committee investigations of the Intelligence Community. After my State Department service, I moved to the staff of the Senate Armed Services Committee where I was the General Counsel under Senator Sam Nunn and his designee to the Senate Intelligence Committee. Later I served as General Counsel of the CIA and have worked closely with the Intelligence Community in my private practice. And, I currently serve on the External Advisory Board of the Director of the Central Intelligence Agency.

56838.241

departments and agencies, but with a singular mission: the provision of intelligence to the President and the execution of intelligence operations. Over the years, many efforts have been made to stitch the "community" into something more. But we've never agreed on what that "more" is.

The attacks of 9/11 starkly demonstrated that the previous system, in which the Director of Central Intelligence was "dual-hatted" as the Director of the CIA and the head of the U.S. Intelligence Community, had serious shortfalls. To address these problems, the 9/11 Commission recommended, among other things, the establishment of a National Intelligence Director who would head the U.S. Intelligence Community. I was a supporter of that legislation and still believe it was the right thing to do.

As this Committee knows, IRTPA gave the DNI broad responsibility, but not clear authority to carry out many of those responsibilities. The result is much confusion and inconsistency between the authorities of the DNI and those already held by others in the Community, including the Secretary of Defense and the Director of CIA.

This confusion over authorities lies at the heart of the problem. Senior officials tell me they spend an inordinate amount of time arguing over these authorities. This creates friction - and occasionally anger - that distracts from the accomplishment of their important missions. More disturbingly, some officers even speak about mistrust among agencies. This must be addressed.

This friction can erupt into unseemly bureaucratic warfare. One widely reported dispute had to be resolved by the White House. In my conversations, several officers said that experience left "scars" that will take a long time to heal.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00436 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.242

The men and women of the United States Intelligence Community are dedicated, hard working, enormously talented individuals. Many risk their lives to keep us safe. By all accounts, they work together extremely well in the field, for example in Iraq and Afghanistan, but for some reason they are not able to find that same ability to work together here in Washington.

The individual elements of the Community regard themselves - correctly - as elite organizations. They have great morale. They take pride in their organizations. Competition to join the Community is fierce. For example, the CIA gets about 180,000 applicants a year, providing a rich pool of talented Americans committed to service. I have been greatly impressed by the young officers with whom I have recently met in the CIA and other agencies. All Americans should be proud of these men and women.

But maintaining an elite organization with high morale requires careful attention. Strong and clear leadership is needed. The support of the President, the Congress, and the American people is critical. The seemingly endless arguments over authorities undermines the unit pride that all agencies in the Intelligence Community require. We owe it to them to fix this.

I would like to use my time this morning to discuss: (1) my specific observations about the current structure under IRTPA, (2) four areas where the DNI's authority should be strengthened or clarified, and (3) a suggestion that a comprehensive review of these issues is needed.

I. Observations about the Current Structure under IRTPA

Overall, the current structure is not working as Congress intended. The 9/11 Commission recognized that the DCI had three jobs: (1) run the CIA, (2) manage the "loose confederation" of the Intelligence Community, (3) and be the "analyst in chief for the government." National

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00437 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.243

Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* 409 (W.W. Norton & Co. 2004). That was, the Commission said, "too many jobs" and no DCI had ever been able to do all three effectively. *Id.* They recommended, and Congress agreed, that a new national director of intelligence should be established with two jobs: (1) "oversee national intelligence centers on specific subjects of interest," *e.g*, the National Counterterrorism Center ("NCTC"), and (2) "manage the national intelligence program and oversee the agencies that contribute to it." *Id.* at 411.

Those are still valid objectives. However, there was also the concern that ODNI would, as government agencies do, grow and become a layer of bureaucracy between the operating elements of the Intelligence Community and the President. Unfortunately, many are convinced that has occurred.

One of the most prescient observations I heard was that we are slowly replicating the problems of the old DCI. Many believe the dual responsibilities of providing intelligence to the President on the one hand and managing the Intelligence Community on the other are sufficiently distinct that they should be separated. In a sense, it's the reason the Goldwater Nichols Act streamlined the chain of command and clarified that the military service chiefs were not to exert operational control of their services in the field. Operational control is to be exercised by the combatant commanders.

But all is not gloom. Each of the gifted Americans who have served as DNI has accomplished a great deal and put many excellent policies and procedures in place. The current DNI, Admiral Blair, has brought extraordinarily talented people into his office and has established very good relationships with the defense agencies, including in the important area of procurement. Support to the warfighters is excellent. Nearly everyone agrees there is much

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00438 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.244

better information sharing within the Community. "A-Space," the research tool for analysts, gets very high marks. NCTC is widely praised as very effective, and there is acceptance that joint duty in more than one agency or discipline should be a requirement for promotion to senior ranks.

But there are also assertions that ODNI often overreaches in its demand for information and micromanages the agencies. There are frequent complaints that the staff of the ODNI is too large and that it relies far too heavily on contractors.

I know, for a fact, that Director Blair does not seek to micromanage or make excessive demands for information. However, he also confronts a mismatch between his statutory responsibilities and his authority to carry them out.

II. Four Areas where the DNI's Authority Should be Strengthened or Clarified

These basic observations lead me to believe that the Director's authority should be strengthened in those areas that are essential to the effective management of the Community and clarified in operational areas where there is overlap and inconsistency.

I would like to discuss four specific areas that I hope will illustrate my observations. In two of them, I believe the Director needs additional authority and in two I believe his authority needs to be clarified.

A. The Role of the Director of National Intelligence

What do we want the DNI to do?

By law, the DNI is to serve "as the head of the intelligence community" and "as the principal advisor to the President . . . for intelligence matters related to the National Security." 50 U.S.C. § 403(b)(1)-(2). There is a considerable amount of discussion among the intelligence

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00439 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.245

agencies as to exactly what that means. Because the relationship between the DNI and the President is so important, I would like to discuss it in some depth.

Section 403-1 says that the Director of National Intelligence shall be "responsible for insuring that National Intelligence is provided . . . to the President." 50 U.S.C. § 403-1. But does this mean that he or she should be the President's daily briefer? Does it mean that the DNI is personally responsible for the production of all intelligence products?

Obviously, this is a matter that must be worked out between the President and his DNI, but it illustrates the challenges of the current statutory scheme. Those who think that the DNI should not be the daily briefer believe the briefer should be a senior intelligence analyst whose only duty is to brief the President and that he or she should bring with them "subject matter experts" when particular subjects are to be discussed. The briefer would then be able to follow up on issues that arise in the briefing and respond to the President in a timely fashion. The DNI should participate in the daily briefing as needed. The demands of being the daily briefer, however, almost surely make it impossible to devote the time needed to carry out effectively his management responsibilities for the broader Intelligence Community.

If the DNI is the daily briefer or is in the Oval Office excessively, it also raises the specter that has occasionally bedeviled the Intelligence Community – namely, that the senior intelligence official of the government should not be drawn into the policy process so deeply that he or she is not able to step back and render fully independent advice to the President. This is a very tricky balance, and does not lend itself to resolution by statute. Clearly, the President must have great confidence in the DNI and the DNI must have unfettered access to the President. However, maintaining a respectable distance seems wise.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00440 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.246

Along these same lines, the DNI has a responsibility that I believe is sometimes overlooked. Just as the Secretary of Defense and the service secretaries have the obligation to insulate the uniformed armed services from the political winds of Washington, so too does the DNI have the responsibility to prevent politics - regardless of its source - from influencing the management of the Intelligence Community, its products, or its operations.

Finally, on the issue of production of intelligence, the career professional analysts who are responsible for the production of intelligence believe, very strongly, that they must be integrally involved in the discussions that lead to the formation and execution of our national security policy. They understand, very clearly, that they are not decision makers, but believe that if they are not "at the table" their ability to provide relevant and useful intelligence is severely degraded. And some have expressed concern that the ODNI structure has placed a layer between them and the decision makers that they believe risks the quality and usefulness of their products.

I wish to emphasize that I do not speak from first-hand knowledge on these matters as I am not an intelligence analyst and have never even been in the Oval Office. However, I do believe these are legitimate concerns and worthy of close examination.

Another concern that arises out of the DNI's basic responsibility is: How much staff is needed to do the job?

There is much talk that the DNI's staff is too large. That is a bit unfair because the staff also includes NCTC, the National Intelligence Council, the National Counter Intelligence Executive, and other organizations that perform vital functions and do so very well. However, in my conversations with elements in the Intelligence Community, I frequently heard that the ODNI staff often micromanages the agencies and engages in duplicative and unnecessary efforts.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00441 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.247

Much of this frustration is with the proliferation of contract employees, not government officials, who "task" the agencies for information. For example, one senior agency official told me that contractors at ODNI had recently requested detailed information about an operation. The agency responded that they were not able to comply with the request because the individuals involved in that operation simply didn't have the time to set aside the mission and respond to the request. The response from the contractors at ODNI was to offer to send another contractor to the agency in order to answer the questions put by the contractors in the first place. This senior agency officer expressed frustration that, to the best of the officer's knowledge, there was not a single government employee "in the loop" with respect to that particular request for data.

Others complain that the requests for information are not coordinated within the ODNI staff and they get conflicting and overlapping requests from different elements of the ODNI staff. Many of these comments were made with considerable passion. Some even said that the Office of the DNI was so intrusive that it was causing harm and getting in the way of good intelligence.

In response, ODNI correctly points out that the Congress has given the Director very clear missions and responsibilities. In many cases, the DNI does not have the direct authority to ensure that these responsibilities are carried out. Therefore, it is necessary to collect a great deal of information so the Director can understand what is happening across the Community and develop and implement policies to carry out the responsibilities he has under the law.

B. Acquisition Authority

The second area where confusion has arisen is the responsibility for acquisition. Here I believe that the DNI needs additional authority, particularly over the large technical collection platforms, most of which are in the Department of Defense ("DOD").

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00442 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.248

There is, as this Committee knows, considerable overlap between the responsibilities of the DNI and the Secretary of Defense. One of the biggest challenges in the massive DOD intelligence procurement programs is to ensure that the requirements are adequately understood, are not overstated, and that the appropriate budgetary and procurement discipline is applied to the programs throughout their life cycle.

With respect to the large programs in the DOD, I note that DNI is responsible for providing "guidance for developing the National Intelligence Program budget" to each agency, 50 U.S.C. § 403-1(c)(1)(A), and "ensur[ing] the effective execution" of that budget. 50 U.S.C. § 403-1(c)(4). Although the Director is given a considerable amount of authority over the "allotment or allocation" of the National Intelligence Program, he still lacks authority to do many of the things that Congress intended him to be able to do. 50 U.S.C. § 403-1(c)(5)(A).

For example, it is not clear to me that he has adequate authority over programs in the National Reconnaissance Office ("NRO"), the National Security Agency ("NSA"), or the National Geospatial Agency ("NGA"). These agencies are part of the DOD, and the Secretary of Defense is required by law only to "ensure appropriate implementation of the policies and resource decisions of the DNI by elements of the Department of Defense within the National Intelligence Program." 50 U.S.C. § 403-5(a)(2). Obviously, the word "appropriate" gives the Secretary of Defense enormous flexibility to decide what to do - or not do. This provision, when coupled with Section 1018 that provides that nothing in the DNI's authority shall "abrogate" the existing statutory authority of any other department head illustrates this problem. 50 U.S.C. § 403 note.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00443 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.249

On a positive note, Director Blair has established a system that is designed to give him oversight without oppressive interference in the execution of these DOD intelligence procurement programs. Both sides, I understand, are very pleased with these new arrangements.

However, there is still confusion over authorities. For example, the law is not clear as to whether the agencies or ODNI are responsible for Independent Cost Estimates and at what threshold. I know the two pending intelligence authorization bills address this and I hope Congress will quickly pass that legislation. Similar confusion persists over re-programming authority that makes it difficult to execute the DNI's priorities during the execution of programs.

The fact that there continues to be confusion in the very important area of procurement suggests to me that a careful review is needed. Over time, DNIs have been able to work out arrangements that sometimes work - but not always. However, the successful arrangements are largely personality-dependent and suggest that the underlying statutory authority should be reviewed to see if adjustments are needed.

C. Information Sharing

A third area where the authorities of the DNI could usefully be strengthened is information sharing. Information sharing has been a focus of this Committee and I commend you for the hard work you have put into this critical issue. The Christmas bomber demonstrated how difficult it is to get this issue right and I'm pleased that the government is working very hard to see what went wrong and to fix the problems.

As you know, I am privileged to serve on the Markle Task Force on National Security in the Information Age, co-chaired by Zoë Baird and Jim Barksdale. Since 2002, the Markle Task Force has pursued a "virtual reorganization of government" that uses the best technology to

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00444 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.250

connect the dots and the best management know-how that gets people working across agency lines to understand the meaning of fragments of information.[2]

Although much has been accomplished, much remains to be done. For example, I understand that the ODNI has "dozens" of bilateral agreements with other agencies that are needed to obtain information within the possession of those other agencies. We still need uniform guidance that enables the Intelligence Community to obtain appropriate access to U.S. person information in a number of diverse data bases.

Technology exists to make the information in all the systems that exist today "discoverable" without creating a large centralized database. When "data can find data" through discoverability, the process of piecing information together can be automated so that an electronic notification is sent to relevant analysts when new information reveals a connection that may warrant action. When discoverability is combined with an authorized use standard that allows users to see what has been discovered based on their specific role or mission, persistent obstacles in the present system of classification and stovepipes can be overcome. Using such a decentralized system of discoverability simultaneously improves security and minimizes privacy risks by avoiding bulk transfers of data.

Shortly before leaving office, Director McConnell issued a directive, Intelligence Community Directive 501, that is being implemented by Director Blair. ICD 501 moved the Community very much in the right direction. We need to press for complete implementation of that directive. The Director must also work very hard to encourage collaboration across all agencies and departments to empower the establishment of ad hoc communities of interest that

[2] The Markle Task Force has released four reports that are available at http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00445 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.251

focus on a given intelligence challenge. The stove pipes are still there and we still have much work to break through them.

My concern is that the DNI may need additional authority to press for these changes. I understand that ODNI and NCTC are currently reviewing whether additional authority is needed. When that review is completed, I hope the President and Congress will give them any additional authority they believe they need.

D. Human Resources

The fourth area where I believe clarification is needed is in the human resource area. As I noted earlier, there is broad agreement that joint duty should be a requirement for promotion to senior rank in the Intelligence Community. This requirement, which is a hallmark success of the Goldwater Nichols Act, assures that officers will understand other elements of the Intelligence Community. It greatly enhances cooperation across the Community and improves both operations and production.

Joint duty is a very noble objective, as are a number of other human resource objectives contained in IRTPA. However, the agencies frequently complain that there seems to be an obsession with uniformity on personnel issues across the Community that is unnecessary and threatens the effectiveness, initiative and unit pride of the various agencies. For example, I understand that ODNI recently has required that a database be created on every employee in the Intelligence Community with eighty fields that must be completed for each individual. As I understand it, the argument is that this data is needed so that ODNI can assure compliance with the law and report accordingly to Congress. Agencies have complained that this creates a great burden and questioned whether it is truly needed. In some cases, particularly those with officers

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00446 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.252

under cover, it creates counterintelligence risks. One must also ask whether the objectives of the law could be achieved without requiring this level of detailed oversight.

III. A Way Forward

Let me now outline some suggestions that I hope will address these issues. Some of these thoughts are tentative and all require more deliberation. But I believe they are worthy of consideration.

A. Goldwater Nichols for the Intelligence Community

I believe a strong Director of National Intelligence with clear authority over policy, procurement, and management of the Intelligence Community is needed. Unfortunately, we now have conflicting authorities and overlapping responsibilities that cause frustration and waste great amounts of time in arguing over those authorities. In the course of my conversations, I heard frequent suggestions that a "Goldwater Nichols" act is needed for the Intelligence Community. I believe there is much merit in that suggestion.

Analogies are never perfect. However, there are approaches in Goldwater Nichols that could be adapted to help with the challenges in managing the Intelligence Community. Keep in mind that the Goldwater Nichols legislation made relatively minor changes - things like streamlining the chain of command, establishing a Vice Chairman of the Joint Chiefs, requiring joint duty for promotion to flag rank, and giving the Chairman the power to choose officers for assignment to the Joint Staff. Accordingly, I would like to make a few suggestions that draw on the success that emerged from our experience with Goldwater Nichols.

Let me begin by discussing the relationship between the CIA and the ODNI, probably the most challenging relationship. That is true for a number of reasons, including the legacy of the CIA and the fact that it is the only agency over which the DNI has clear authority. The other

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00447 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.253

agencies are all part of another cabinet department and Section 1018 gives those departments a handy tool anytime they wish to ignore the DNI's directions.

Section 1018 speaks only in terms of "department" heads and some have suggested that CIA should be put on the same footing by adding the word "agencies." I believe that Section 1018 should be carefully reviewed. A strong case can be made that it should be repealed, but if it is to stay in the law, I believe consideration should be given to including the word "agencies" so that CIA is treated like other agencies in the Intelligence Community. A further complication is the language in IRTPA that says the Director of CIA "shall report to the DNI regarding the activities of the CIA." This language should not be studied in the war colleges as a model for establishing clear lines of command and control.

The CIA was established to be "central" and to be independent. In my view, those functions are still critical. CIA is the only member of the Intelligence Community that is not part of another department. No other agency has broad responsibility for all-source production of intelligence. The analysts at CIA have developed, over the years, a close working relationship with the National Clandestine Service that is critical for assuring that human intelligence ("HUMINT"), which is often the most valuable intelligence, is adequately factored into the final product.

It is occasionally frustrating to DNIs that the President and the National Security Council ("NSC") continue to deal directly with CIA rather than going through them. That frustration is understandable, but it is also easy to understand why the President and the NSC reach out directly to CIA.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00448 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.254

CIA is, after all, the chief operational arm of the Intelligence Community. Therefore, the wise approach may be to tailor the authorities to maximize the value of the CIA and, where necessary, clarify and strengthen the management responsibilities of the DNI.

In Goldwater Nichols terms, perhaps we should think of the CIA as a "combatant command" responsible for production of all source intelligence to the President, covert operations, and HUMINT. The "chain of command" for intelligence activities would run from the President through the Director of National Intelligence to the Director of CIA. Certain other intelligence agencies, for example NSA, NGA, and NRO could be thought of as "combat support agencies" supporting the CIA in its national mission, much as they support the regional combatant commands in the DOD. To continue the analogy, the DNI would function a bit like the Chairman of the Joint Chiefs of Staff in that the chain of command would pass through him to the Director of CIA, but the execution of the mission would rest with the Director of CIA. The DNI should be able to choose his own staff, much as the Chairman of the Joint Chiefs does. The DNI would also function a bit like the Secretary of Defense in that he has responsibility for management and overall policy of the Community. The DNI should have clear authority to appoint - and remove - heads of the agencies that comprise the Intelligence Community.

But much as the President deals directly with his field combatant commanders, it is reasonable, and one can argue desirable, for the President to deal directly with the Director of CIA.

A more difficult organizational challenge is represented with respect to the issue of domestic intelligence. Much progress has been made in integrating the foreign intelligence agencies and the FBI. And the FBI has made great strides in developing a genuine domestic intelligence function. However, I remain concerned that we still don't have the organizational

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00449 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.255

structure right. In preparing for this hearing, I concentrated on the foreign side of the house, but I believe many of the observations I've made may well apply to the domestic side. Should, for example, we begin to think of the National Security Branch ("NSB") of the FBI as the "combatant commander" for counterintelligence and domestic intelligence? Do we need to establish the NSB as a free-standing domestic intelligence service, perhaps in the Department of Justice or Homeland Security? These are very difficult questions and raise some fundamental issues about how domestic intelligence should be conducted in our democracy, but I believe we must keep asking them.

B. Review of IRTPA

Mr. Chairman, many of the organizational challenges that arose after the creation of the DNI have been worked out; for example in the revision of Executive Order 12333 issued in 2008 and in numerous DNI directives. Nevertheless, much tension remains. Some of the remaining issues can be solved by strong presidential leadership. However, I also believe the statute should be reviewed to address some of the ambiguity and confusion that I've discussed today. I believe it should be possible to develop a clearer division of responsibility between the DNI and the elements of the Community that will improve the management of the Community while preserving the special nature and effectiveness that each agency in the Community rightfully takes pride in. The result should be, if we get it right, a great improvement in the quality of the intelligence provided to the President and, at the same time, a great improvement in the management and effectiveness of the Community.

Many senior officers in the community put it this way: "The DNI should establish clear policies, provide direction and priorities for collection, develop integration strategies and assure that requirements for the major acquisition programs are sound. But the execution must be left

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00450 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.256

to the agencies who are the operating arms. The DNI must have authority to hold me accountable, but he should not micromanage. Just give me a mission and let me do it. If I fail, fire me." That seems right to me.

C. Establishment of a Separate National Intelligence Program

As part of this review, consideration should be given to the establishment of a separate National Intelligence Program ("NIP"). This would be a very dramatic change from the current practice and would require much thought - and political compromise in the executive and congressional branches. But its time may have come, especially given the procurement concerns discussed above. As a separate budget program the NIP would be authorized by the two intelligence committees, with appropriate sequential referrals to the other relevant committees for authorization of their portions. It would then be appropriated as a separate appropriation. The top line would necessarily be unclassified and a new congressional rule may have to be adopted to assure that it could be debated and considered in a manner that protects classified information and prohibits politicizing the budget. By that I mean it would not be advisable for the intelligence budget to become like the defense budget where individual members of Congress seek to amend the authorization of appropriation bills to favor constituent contractors.

I understand that the administration is exploring ways to have the intelligence budget separately treated within the existing structure. I encourage that but it may be necessary to go even further. I fully recognize that a wholly separate NIP would be a sea change in the manner in which intelligence agencies are funded and managed. And I recognize how hard it would be to achieve this. However, I believe it should be closely examined. Even if we conclude such a change is not advisable, the process of thinking it through will, in all likelihood, shed light on

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00451 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.257

some of the more difficult management problems, and creative solutions may emerge that would not otherwise have occurred to us.

D. Next Steps

There are, in my view, three basic approaches to a review of IRTPA and the Intelligence Community organization. Congress could take the lead, perhaps by setting up a special task force of members from the relevant committees. The President could order the study on his own, perhaps using the President's Intelligence Advisory Board. A third approach would be for the President and Congress to encourage an outside group, such as the Bipartisan Policy Center to conduct the study. As the Committee knows, Governor Keane and Mr. Hamilton have a strong interest in this subject and have scheduled a conference on the matter on April 6.

Regardless, I believe a review should be done and done now. I thank the Committee again for its leadership and the opportunity to appear before you this morning.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00452 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.258

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the Senate Committee on Homeland Security and Governmental Affairs

"THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: INTELLIGENCE REFORM AND INTERAGENCY INTEGRATION"

A Statement by

Rick "Ozzie" Nelson

Senior Fellow and Director, Homeland Security and Counterterrorism Program

Center for Strategic and International Studies (CSIS)

March 17, 2010

Dirksen Senate Office Building

1800 K STREET NW, WASHINGTON DC 20006 | P. 202.887.0200 F. 202.775.3199 | WWW.CSIS.ORG

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00453 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.259

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Chairman Lieberman, Ranking Member Collins, distinguished members of the committee, thank you for the opportunity to discuss this important topic.

I come to you today as a retired Navy Officer with over twenty years of operational and intelligence experience. I spent most of the last decade focusing on the challenges of combating global terrorism, including assignments at the National Counterterrorism Center (NCTC), the National Security Council (NSC), and the U.S. Special Operations Command. In 2005, I was selected to serve as one of the original planners in NCTC's Directorate of Strategic and Operational Planning and was a lead planner for the nation's inaugural National Implementation Plan for Counterterrorism (NIP), approved by President Bush in June, 2006. During the next few minutes, I plan to discuss NCTC and its legislatively-mandated role to conduct strategic operational planning.

Background:

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) addressed serious weaknesses in our nation's intelligence community and its ability to combat terrorism. In creating the Directorate of National Intelligence (DNI) and NCTC, the landmark legislation sought to improve collaboration among the numerous departments and agencies that deal with threats to our nation's security. Among the Act's most significant contributions was its recognition that the our nation's Cold War national security organization was no longer sufficient to address the complex and myriad transnational threats that we will face in the 21st Century. To these ends, DNI has embarked on its mission to better integrate the Intelligence Community and NCTC represents an unprecedented recognition of the need for the United States government to focus on security beyond the traditional threats posed by nation-states.

As with any innovative idea, achieving the aims of this legislation will come through evolution. Valuable lessons can and should be learned when ideas and concepts meet implementation. Those lessons should be leveraged to improve upon the original ideas and ensure the vision of its creators is being met. This is the case with NCTC and particularly with the Directorate of Strategic Operational Planning (DSOP).

Why do we need a stronger, more effective DSOP? In short, while numerous departments and agencies work aggressively to counter threats as they emerge, the Intelligence Community, and arguably the government as a whole, still lacks a truly "inter-active" process for addressing terrorism. One need look no further than the failure to "connect the dots" prior to the December 25 plot to understand why coordination is so important. Furthermore, because so much effort is channeled toward the immediate exigencies of the day, the government has not devoted sufficient time to long-range thinking about how to develop a common—and ultimately, strategic—framework for dealing with terrorism and other sub-state, transnational threats. The issue will grow more complex as enhanced collaboration with state and local governments—as well as with the private sector—becomes even more necessary in a globalized world that blurs national borders and lines between public and private domains. To ensure our security in the coming decades, then, interagency coordination mechanisms like DSOP must be strengthened. And achieving this goal will require legislative and institutional changes.

1800 K STREET NW, WASHINGTON DC 20006 | P. 202.887.0200 F. 202.775.3199 | WWW.CSIS.ORG

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00454 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.260

To be fair, I last served at NCTC in 2007, but as a "plank holder" and someone committed to the success of DSOP, I have continued to follow the organization though the years. The organization has evolved and its personnel are dedicated individuals with some of the most difficult and grinding jobs in the United States government. After all, coordinating and integrating the nation's counterterrorism programs across more than 16 departments and agencies is a formidable challenge, particularly with so little margin for error.

DSOP has experienced success in many noteworthy areas. The NIP is a remarkable achievement given the document's size and complexity, along with the fact that it must navigate between agencies and be signed by the president. And arguably, DSOP remains one of the few places in the government where interagency planning takes place. Most importantly, is has become the de facto incubator for the government's interagency planners. This is why it must succeed.

Enhancements to DSOP must address three key areas: mission, authorities, and personnel. DSOP's mission must be refocused to ensure its role in and value to the interagency CT architecture is understood. Specifically, the "strategic operational" planning requirements must be divided into two separate planning functions. DSOP should have distinct strategic and operational roles. In its strategic role it should be the government's primary force behind CT policy, strategy, and resource allocation. In its operational role it should be leading near-term planning efforts against terrorist groups, serving as the leader, integrator, and arbiter for CT plans. It should build and house the nation's premiere CT planning capability.

DSOP's operational authorities should not be increased; however, interagency CT authorities and responsibilities must be clarified. IRTPA gave DSOP the authorities to conduct its specific mission, yet no authorities were taken from any other department or agency in support of DSOP's creation. Not only did this create overlapping authorities, but it also established no compelling reason for departments and agencies to participate in the DSOP process, as they could continue their counterterrorism efforts under extant powers. These overlapping areas of responsibility must be clarified. Without this, departments and agencies will continue to spend time fighting turf battles when they should be focused solely on the enemy at hand.

And last, DSOP should be given the personnel to conduct its mission. This does not necessarily mean more people; it means the right people. If NCTC is going to lead the government's CT efforts, it must possess the nation's best and brightest CT minds from across the government. Currently, the organization faces a dilemma where an ambiguous mission and unclear authorities keep DSOP from attracting and retaining the requisite personnel; this lack of appropriate personnel keeps it from executing a clear, well-defined mission. Much of this cycle is driven by the lack of interagency support for DSOP and it remains a significant impediment to DSOP's success.

Below, I outline in greater detail the three most important factors in determining DSOP's success: mission, authorities, and personnel.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00455 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.261

Mission:

DSOP's IRTPA-mandated mission is clear in theory, but convoluted in practice. DSOP was given the broad guidance to "conduct strategic operational planning for counterterrorism activities integrating all instruments of national power" and to "assign roles and responsibilities" for CT activities. The intent was for DSOP to fill the void in counterterrorism planning between strategic level policymaking and tactical level operational activities. This chartered DSOP to not only fill the vertical gap between the strategic and tactical, but also to bridge the horizontal planning gap in the interagency between departments and agencies.

In an attempt to close this gap, the term "strategic operational" planning was created and tasked to DSOP. The conflating of the terms "strategic" and "operational" has hindered DSOP since its inception and remains a significant problem. These are terms of art and those with background in planning understand clearly that they are separate and unique requirements. By merging these terms, DSOP is stranded in a "planning no man's land" between high-level policy and strategy development and operational and tactical level planning. The impact of DSOP's planning efforts is uncertain to many in the interagency as plans are developed and then followed-up with little implementation or assessment oversight. As a result, DSOP's function and relevance remain unclear to many, and the organization continues to experience difficulty in defining a planning output and an attendant review process that are acceptable to the interagency.

We have a chance to refocus DSOP's mission before the status quo becomes ingrained and irreversible. To do so DSOP should split into two distinct sub-sections: a branch that focuses on strategic plans and one that focuses on operational plans. This would immediately clarify NCTC's role. It also helps determine the required personnel resources, as strategic and tactical planners will possess vastly different backgrounds and skill sets.

The strategic part of DSOP should focus on high level CT policy, strategy, and resource allocation. It should lead the interagency policy- and strategy-making efforts, including those that require White House approval. In this capacity, it would not only guide and develop policies required to posture the government for terrorist threats, but also serve as an arbiter between departments and agencies. This element also would have an enhanced and more assertive role in resource allocation and drive the primary input to the Office of Management and Budget (OMB) for resource CT prioritization and investments. While this mandate currently exists, DSOP's role should be strengthened and enhanced to ensure that requirements are tied to strategic outcomes.

The lowest ranking entity that should have veto authority over NCTC strategic level efforts is the National Security Council or an NSC Principals Committee. Of course, such a role will require a uniquely skilled cadre of planners that currently is not fully present at NCTC. But by clearly defining this requirement, a requirement clearer than "strategic operational planner," the capability can be more easily filled and developed. Such a clear strategic role will empower NCTC as the lead government strategic CT

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00456 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.262

planning element. And its role in resource allocation will encourage interagency participation in its processes.

A second part of DSOP should focus on operational plans against terrorist groups. Such a construct provides attainable goals—defeat of a group—and allows for ease of implementation. The functional approach of the NIP should be amended so that it can be executed geographically against identified groups. Whether justifiable or not, the Cold War-based national security infrastructure executes geographically, not functionally. U.S. efforts against these groups should be prioritized within the DSOP interagency process, with NCTC serving as the interagency arbiter, in close coordination with the National Security Council.

And finally, to be effective, NCTC and DSOP must be able to credibly measure the results of the plans that the organizations formulate and help to implement. Evaluation and assessment are imperative for DSOP and the government writ large. Policies cannot be readjusted, plans cannot be updated, and resources cannot be reallocated, unless one knows what does and does not work.

Authorities:

The question of authorities is raised regularly in discussions regarding DSOP. The recent Project on National Security Reform (PNSR) study on DSOP offers a comprehensive assessment of this issue. Its comparison of authorities between the Office of National Drug Control Policy (ONDCP), DNI, and DSOP—three similarly chartered organizations—highlights the disadvantage from which DSOP operates and notes that DSOP is the only entity of the three "without authority over people or money."

Many cite DSOP's explicit prohibition from directing operations as a key reason for its struggles, with some calling for empowering DSOP with additional operational authorities. This should not be done, as DSOP lacks the capability and capacity to assume such a role and would fall short of expectations. Any changes to operational authorities must be made in conjunction with wholesale revisions to the entire United States CT apparatus.

With no authority over personnel, resources or operations, DSOP has a limited ability to compel interagency participation and thus remains a relatively powerless organization. There is no "penalty" to interagency entities that decide not to participate in NCTC planning processes. This ultimately hinders DSOP's ability to develop effective CT policy, implement plans, influence operations, and assess progress. It also relegates DSOP to the unenviable role of leading process-orientated approaches to substantive problems. Departments and agencies that actually control operations, personnel and resources address substantive CT problems under their own authorities and well beyond the control of NCTC. This fundamental disconnect marginalizes DSOP's role in the CT community.

What interagency power DSOP does possess comes directly from its relationship with the National Security Council staff and, ultimately, the president. This relationship, codified in IRTPA, remains DSOP's primary source of authority and has been critical in preserving its role in the counterterrorism

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00457 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.263

enterprise. However, the definition of this relationship is personality dependent. And DSOP's ability to drive interagency planning is based on the ebb and flow of guidance from the NSC. As a result, some view DSOP's de facto role as a simple staff extension of the NSC. This role is useful, but limiting, as it keeps NCTC from truly becoming the leading national counterterrorism planning entity. It also subjects DSOP to the exigencies of the day and weakens NCTC independence.

To solve this problem the authorities issue must be addressed across the entire government CT enterprise. As recommended in the PNSR report, the president and Congress should both undertake efforts to evaluate the full scope of the CT enterprise and codify roles and missions across the interagency community. Part of this effort would include clarifying DSOP's mission and authorities.

Specific to DSOP, it should be given authority to influence both resources and personnel. I will discuss personnel in a few moments. Regarding resources, DSOP should be given some authority to control and allocate funds to the various departments and agencies involved in counterterrorism. This would not mean, for instance, that DSOP would fully control federal allocations to these entities. But it would give DSOP a powerful lever by which to incentivize interagency cooperation; quite simply, the departments and agencies that took an active, productive role in the interagency planning process would have a greater say in budget allocations. This authority also would provide DSOP with a dynamic process to adapt both strategic and operational plans to the ever evolving terrorist threat.

Personnel:

The issue of personnel remains a significant factor limiting the evolution and ultimate effectiveness of DSOP. To succeed NCTC must have the right talent. A clear mission with ample authority rings hollow if the appropriate personnel are not brought together to execute what is required.

DSOP has been hindered by the lack of planning talent since in its inception. Unlike its analytic and knowledge management counterparts in NCTC, no standing cadre of interagency counterterrorism planners existed from which a terrorism specific capability could be created. When NCTC's Directorate of Intelligence was created, it was able to pull from a large collection of trained personnel skilled and experienced in basic analytic techniques and, to a lesser degree, interagency collaboration under the legacy Intelligence Community rubric. The same held true for the knowledge management personnel whose technology and data basing skills were directly transferrable to NCTC's mission. This was not the case for DSOP. Few departments and agencies conducted strategic or operational planning and those that did utilized very different models. This made it even more difficult for NCTC to design its planning products. Not only did they lack planners internally who understood plan design, but also the interagency as a whole did not understand or embrace the need for comprehensive planning efforts. This problem—the lack of an interagency planning model or culture—still exists today.

While the process of building this capacity has begun, it has been slowed by two key factors—lack of interagency participation and high personnel turnover.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00458 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.264

First, the interagency must become fully invested in NCTC and the DSOP concept. Being fully invested includes not only recognizing and embracing DSOP's missions and authorities but also, and most importantly, detailing the appropriate number and type of personnel to DSOP, and ensuring robust participation in DSOP planning efforts. The old adage that "plans are nothing; planning is everything" is only valid when those that are conducting the planning are actually involved in the execution of those plans. Since DSOP does not execute plans, it is imperative that its efforts include robust participation by those departments and agencies that have CT implementation authorities. This has not been the case to date and is very problematic.

To address this issue, the interagency must be compelled to participate. While the Goldwater-Nichols Act is a sometimes over-used example, it demonstrates the effect legislation can have in mandating coordination across disparate departments. Congress must pursue legislation that compels the interagency to participate fully in DSOP's process, including obligating personnel resources. Such a commitment to interagency planning is required if the government is going to be equipped to address the proliferation of transnational threats.

Participation in interagency planning entities such as DSOP must be made a part of both the government's and Intelligence Community's human capital system. Personnel, particularly those with operational experience, must be rewarded through pay and promotion incentives to serve in such entities as DSOP. As with Goldwater-Nichols, only radical legislative reform will break down bureaucratic resistance and change the government's approach to these issues.

Second, personnel turnover at DSOP must be limited. This will occur in part by changing the perceptions regarding the value and credibility of DSOP through mission and authority refinement. Beyond this, the government in general and DNI/NCTC specifically must design a standing career pipeline for interagency CT planners. This will incentivize talent to pursue careers in interagency planning and assignment to interagency organizations such as DSOP. A true and credible planning element would in turn produce better strategies and draft and implement more effective plans. This level and culture of interagency planning is required to drive and ensure operational cooperation. As the December 25 plot demonstrated, the global terrorist threat demands this type of collaboration.

I would be happy to elaborate on this and other issues during questions. Thank you, again, for inviting me to speak today, and I look forward to your questions.

1800 K Street NW, Washington DC 20006 | P. 202.887.0200 F. 202.775.3199 | www.csis.org

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00459 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.265

Post-Hearing Questions for the Record
Submitted to the Honorable Jeffrey H. Smith
From Senator Susan M. Collins

"The Lessons and Implications of the Christmas Day Attack:
Intelligence Reform and Interagency Integration"
March 17, 2010

1. In the Intelligence Reform Act, we gave the DNI fairly significant authority over DoD acquisitions of "major systems" funded by the NIP. In fact, the DNI and the Secretary of Defense serve as joint milestone decision authorities to judge the progress of these programs against their management plans.

   Following passage of the Intelligence Reform Act, Congress added a requirement for "major systems" acquisitions in the Intelligence Community: namely that the DNI produce an independent cost estimate before seeking funding for a "major system" acquisition when the full-life cycle cost of the program exceeds $500,000,000. For "major systems" to be acquired by an element of the Intelligence Community within DoD, the cost estimate must be prepared by an entity jointly designated by the Secretary of Defense and DNI.

   This joint designation authority was important so that the DNI could insist on the entity that would perform the cost estimate, instead of relying on a cost estimate produced by the program manager for the major system. These program manager cost estimates have historically underestimated the cost of these systems, often leading to explosive cost growth in programs.

   What has been the difficulty in implementing this provision?

The response to this Question for the Record was not received at time of printing.

56838.379

Opening Statement of Chairman Joseph I. Lieberman
Lessons and Implications of the Christmas Day Attack:
Securing the Visa Process.
April 21, 2010 Hearing

This is the fifth in a series of hearings our Committee has held to examine our intelligence and security systems that – despite all we've done to strengthen them – allowed Umar Farouk Abdulmutallab to board a U.S.-bound airliner and attempt to blow it out of the sky over Detroit last Christmas Day.

I want to welcome our witnesses here today, each of whom has a critical role to play in helping ensure that this type of failure does not happen again. I'd also say, each of whom has become quite familiar to our committee.

The purpose of this hearing is to review the enhancements to our visa security system that have been made over the last few years, the last five years particularly, but specifically to get a progress report on enhancements that have been put in place post-Christmas Day, including changes in how the State Department processes and disseminates information it receives about terrorism in its consulates abroad, and also to have a good discussion about what additional changes may be needed.

The failures that allowed Abdulmutallab to board Northwest Flight 253 are by now familiar to us all: warnings from the father which went unheeded, threats from Yemen which were not run to ground, and information in different databases that was still not connected.

However, one of the most frustrating failures was one that would seem to have been easiest to avoid, which is the misspelling of Abdulmutallab's name during a check of the State Department's visa database, which led the government to believe that he did not have a visa and so did not pose an immediate threat.

I think we all need to understand that, while America has been and remains probably an open country that welcomes visitors, international travel is a privilege in our time and not an absolute, unlimited right.

My concerns about the security of the visa process were one of the reasons that we advocated giving the Department of Homeland Security more authority over the visa-issuing process during the debate and legislative action during which we actually created the department. The events of Christmas Day, I must say, have brought me back to some of those ideas.

Nine years after September 11th we still do not have an automated system in place to check for revoked visas as individuals board airplanes.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00461 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.266

I understand that State and DHS are working to accomplish this in an expeditious manner and I hope to hear reports on that today.

When the Department of Homeland Security was created, Congress- as an another example of the overlap of the two departments and what we can do to deepen it and expedite it- Congress included a provision establishing the Visa Security Program, and giving DHS the authority to set visa policy, and to deploy law enforcement officers to consulates in order to oversee the visa-issuing process because of its post-9/11-added security dimension.

The idea was to ensure that security considerations were given the weight they deserve in visa-issuance. Eight years later, I'm sorry to come to the conclusion that the program has not been a priority for either department. I'd like the witnesses to comment on that.

Here's why I reach that conclusion: DHS and the State Department have identified 57 high-risk consular posts around the world- that's out of a total of 200 posts that issue visas. But only 14 of those have received, or had stood-up in them, Visa Security Program offices.

The President's fiscal year 2011 budget submission does not include any new money for continuing to expand this vital program.

I understand that one of the main impediments to expanding the program, aside from funding, has been reluctance by some of our ambassadors to allow the Visa Security Program offices to be established at their posts, and I'd like to hear about that if that is true.

I gather on at least seven separate occasions, ambassadors have told the Department of Homeland Security that they would not support expansion of the VSP at their embassy.

And some of those posts are ones that are really key in fighting against terror, such as the United Kingdom, Turkey and Indonesia.

It was not our intention when we put this provision in The Homeland Security Act to give ambassadors veto power over this important program.

So, I look forward to hearing from the witness and to working with DHS and DOS and our colleagues on Foreign Relations to ensure that the VSP program does move forward.

Finally, I am heartened that, for travelers from Visa Waiver countries, the Department of Homeland Security has now fully implemented the Electronic System for Travel Authorization – which is known as ESTA – and is making progress in

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00462 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.267

signing the international information sharing agreements that are required by law. That's a significant accomplishment.

The Christmas Day attack- attempted attack- has underlined for us all the importance of effectively sharing information. I believe that expanding this information sharing to include our allies should be one of the Department of Homeland Security's main priorities moving forward, and so I hope the Department will expedite implementation of the agreements to ensure that information is being shared in real time.

Securing our homeland is now really a global enterprise. It begins well before people come to the United States, and that's why it's so important that State and Homeland Security are working closely and effectively together.

Senator Collins?

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00463 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.268

Opening Statement of
Senator Susan M. Collins

"The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process"

Committee on Homeland Security and Governmental Affairs
April 21, 2010

★ ★ ★

Today's hearing will examine the fundamental question of why the Christmas Day bomber, Umar Farouk Abdulmutallab, was allowed to retain his visa, even after his father had informed the American Embassy in Nigeria of his Islamist extremist connections.

From my perspective, the State Department had sufficient information to revoke Abdulmutallab's visa. State Department officials already had decided to question him about his ties to extremists if he chose to *renew* his visa. That he could have been deemed a threat to the United States in the *future* based on his extremist ties, but not a sufficient *current* threat defies both logic and common sense. Had the State Department taken this action, it would have prevented him from traveling to the United States. This was a missed opportunity to stop the terrorist more than a month before his flight.

At the very least, Abdulmutallab should have been required to come to an embassy and explain his activities before he was allowed to travel to the United States. The State Department has this authority. In fact, the Intelligence Reform Act protects the Department from lawsuits when its officials revoke a visa for a visa holder overseas. But the State Department failed to act.

Visa holders with possible connections to terrorism should shoulder the burden of proving they do not intend to harm this nation or its citizens. If they cannot meet this burden, then we cannot take the risk of permitting them the privilege of traveling to our country.

Following the attempted attack on Christmas, the Intelligence Community has reviewed the visas of all persons listed in the broadest terrorist database, known as TIDE, to determine whether or not they should be permitted to retain their visas. In my judgment, they should keep their visas only in exceptional circumstances that are carefully considered by the State Department, Intelligence Community, and Department of Justice.

56838.269

Essential policy questions include: Is there now an ongoing policy to check the TIDE list for individuals who hold U.S. visas? What is the Administration's current policy on the revocation of the visas held by these individuals? What is the policy on visa revocation for individuals on the terrorist watchlist?

Revoking the visas of suspected terrorists is, however, only the first step. The Department of Homeland Security also should confirm the validity of the visa of every foreign passenger who attempts to board an airplane to this country rather than waiting until his arrival in our country. There does not appear to be a technological barrier since DHS already confirms whether a passenger is on the No Fly or Selectee list in this manner.

I also want to know how the State Department will ensure that minor misspellings do not prevent its officers from discovering immediately that a suspected terrorist has a valid visa, as initially happened with Abdulmutallab. Computer algorithms have been around for decades that can find close name matches to uncover a misspelling, and the State Department should expeditiously adopt such tools.

In general, the Department of Homeland Security must provide greater oversight of the visa issuance and revocation process, as it was authorized to do in the Homeland Security Act of 2002. That Act required DHS to deploy trained visa security officers to overseas consular posts, but DHS has only reached 14 of the 57 high-priority foreign posts – with plans to reach another four. Why has the joint effort of DHS and the State Department to expand this program been so slow?

One important way that DHS is enhancing the security of the visa process is through the implementation of a requirement that Visa Waiver Program travelers receive an electronic travel authorization by providing information to DHS for vetting in advance of travel. This additional step should add a security layer for travelers from countries that currently are not required to obtain a visa.

As we know, terrorists will continue to seek to exploit any vulnerabilities in our visa system. We must continue to strengthen our visa issuance and revocation process. Since this is a primary means of preventing terrorists from traveling to our nation, it must work effectively.

56838.270

TESTIMONY

OF

DAVID HEYMAN
ASSISTANT SECRETARY - POLICY

U.S. DEPARTMENT OF HOMELAND SECURITY

Chairman Lieberman, Senator Collins and other distinguished Members, thank you for the opportunity to appear before the Committee to discuss the Department of Homeland Security's (DHS) work in the area of promoting and overseeing secure travel to the United States.

Targeting terrorist travel is one of the most powerful weapons we have to counter the ability of terrorists to operate. Travel security begins with international travelers obtaining legitimate identity documents from national authorities. Should a visa be needed, the international traveler applies for one at a U.S. Embassy or Consulate and undergoes a personal interview and checks against law enforcement, terrorism, and immigration databases. Travel security also includes passenger and baggage screening, before and during travel, flight security through air marshals, hardened cockpit doors, as well as other measures. Finally, it includes passport control and customs and immigration inspection upon arrival (or prior to departure in certain locations). Every step along this pathway presents a vulnerability to would-be attackers, who must come out of the shadows and interact with security personnel at ports of entry and abroad.

Foreign travelers to the United States come to the attention of U.S. officials either by applying for a visa at a U.S. Embassy or Consulate or by traveling to the United States under a visa-free program, one of which, the Visa Waiver Program (VWP), requires advance authorization to travel. The Department of State is responsible for the day-to-day operations of visa issuance. DHS' role in visa policy and guidance is outlined in Section 428 of the Homeland Security Act of 2002 (HSA), which gives the Secretary of Homeland Security the authority to issue regulations with respect to the granting or refusal of visas. The attempted attack by Umar Farouk Abdulmutallab on December 25, 2009, was one more reminder of the importance of ensuring that visa screening procedures utilize tools to counter terrorism; to that end, screening must include functionally related measures such as document verification capabilities and enhanced international information sharing. Taken as a whole, these procedures help ensure not only the integrity of our borders and immigration system, but also the security of the traveling public and the global air transportation system.

The first part of travel security is the authorization step, which is the focus of this hearing. My colleague, Assistant Secretary John Morton, U.S. Immigration and Customs Enforcement (ICE), will testify on DHS' Visa Security Program and other DHS initiatives to effectively screen large numbers of individuals well in advance of travel to the United States. Ambassador Janice Jacobs, Assistant Secretary for Consular Affairs at the Department of State, will discuss the visa issuance process. For my part, I will limit my testimony to the VWP, the program administered by DHS under Section 217 of the Immigration and Nationality Act (INA), as amended. The VWP currently allows citizens from 36 countries to travel to the United States without a visa and, if admitted, to remain in our country for a maximum of 90 days for tourist or business purposes.

56838.271

Some have argued that travel under the VWP carries inherent and inevitable risks not found in visa travel. We would argue that the VWP drives international travel security initiatives and enhances law enforcement and security cooperation with foreign governments while promoting legitimate trade and travel. I will elaborate on the merits and security value of the program in several critical respects throughout this hearing.

Today I would like to: 1) provide a brief overview of the VWP's security benefits; 2) discuss how DHS and its partners are working with VWP countries to ensure their compliance with the information sharing requirements of the "*Implementing Recommendations of the 9/11 Commission Act of 2007*" (9/11 Act); 3) highlight our progress to date in that endeavor—along with some of the remaining challenges; 4) provide an update on our efforts to evaluate the overstay rates of VWP countries; and 5) outline where we see the program going in the future.

I) VWP Security Benefits

The VWP is an important tool for increasing security standards, advancing information sharing, strengthening international partnerships, and promoting legitimate trade and travel to the United States. The VWP was first authorized by Congress as a pilot program in 1986 to facilitate low-risk travel to the United States, boost international trade and cultural links, and promote more efficient use of consular resources. Since the program's inception, Congress and the Executive Branch have worked together to implement a number of security enhancements. Immediately after 9/11, for example, new requirements were put in place to tighten passport security standards and increase the frequency in which countries are formally reviewed for their designation status.

The 9/11 Act transformed the VWP from a program that evaluated security threats broadly on a country-by-country basis into one that has the added capability to screen individual travelers for potential threats that they may pose to the security or welfare of the United States and its citizens. In addition, the 9/11 Act mandated more robust information sharing between the United States and its VWP partners. Since the passage of the 9/11 Act, DHS and its partner agencies have worked diligently to implement the new requirements.

Some have also argued that the program has deficient security measures in place and that each individual VWP country's security risks need to be thoroughly reviewed. In fact, because of the 9/11 Act and pre-existing statutes, that's exactly what we are doing. DHS, for example—in cooperation with other departments and agencies—conducts intensive biennial reviews of VWP countries. Often these reviews include site-visits to the country being evaluated so that DHS can observe, among other things, the country's border and passport security procedures.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00467 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.272

A critical innovation of the 9/11 Act was the requirement for the Electronic System for Travel Authorization (ESTA), which allows for the pre-travel and recurrent screening of VWP travelers to the United States. Since ESTA became mandatory for all VWP travelers in January 2009, DHS has taken a measured approach to ESTA compliance and has worked to make the implementation of ESTA as smooth as possible for VWP partners, travelers, and stakeholders. In January 2010, DHS transitioned from informed compliance to enforced compliance for ESTA. This transition focused on repeat offenders—those travelers who have previously arrived at a U.S. port of entry under the VWP without an ESTA approval. DHS informed air carriers that effective March 20, 2010, they would be subject to significant administrative fines for carrying non-compliant ESTA passengers to the United States.

The ESTA screening process is providing tangible security benefits, such as identifying matches to the Terrorist Screening Database maintained by the Federal Bureau of Investigation's Terrorist Screening Center (TSC) and more than 5,700 lost or stolen passport (LASP) matches. ESTA provides DHS with the capability to conduct advance screening of VWP travelers. This is critical because it enables DHS to preclude some travelers who are ineligible for the VWP from initiating travel to the United States. Travelers whose ESTAs are denied must undergo the visa application process.

As of April 7, 2010, more than 18 million ESTA applications have been processed. In most cases (more than 99.5 percent overall), ESTA provides an immediate determination of eligibility for travel under the VWP. Overall compliance by VWP travelers is extremely high. Notably, since DHS transitioned from informed to enforced compliance in the last three months, the average ESTA daily compliance rate for all VWP travelers has increased by approximately six percent and is likely to continue to increase. The ESTA compliance rate is currently above 97 percent.

The security benefits of the VWP are many and mutually reinforcing. The VWP requires bilateral information sharing arrangements regarding the exchange of terrorism screening information and the possible perpetrators of other serious crimes, as well as the sharing of LASP information. Moreover, there are higher standards for transportation security, aviation security, border security, and document integrity for VWP countries than for countries that do not participate in the program. DHS, with the support of the Departments of State and Justice and the Intelligence Community, reviews these standards and capabilities on a regular basis as a condition for continuing designation in the program. No other mechanism provides DHS with the opportunity to regularly conduct as broad and consequential inspections of foreign security standards as does the VWP.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00468 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.273

It is important to note that DHS conducted such inspections well before the 12/25 incident and we will continue to do so. To complement these efforts, DHS has developed a continuous and vigorous monitoring process to ensure awareness of changing conditions in VWP countries, including regular communication with the relevant U.S. and foreign embassies for updates of law enforcement or security concerns related to the VWP.

II) Status of VWP Information-Sharing Agreements

Overview

The 9/11 Act requires that VWP countries enter into agreements with the United States to share information regarding whether citizens and nationals of the country represent a threat to the security or welfare of the United States and its citizens, and information on LASPs. This emphasis on information sharing with trusted international partners is especially critical in the aftermath of the failed terrorist attempt to bring down Northwest Flight 253 on December 25, 2009.

DHS, with the support of the interagency, has determined that the preferred mechanisms to meet the information sharing requirements with VWP countries, per the 9/11 Act, include: a bilateral Homeland Security Presidential Directive-6 (HSPD-6) arrangement to exchange terrorism screening information; a bilateral Preventing and Combating Serious Crime (PCSC) Agreement to exchange information on possible perpetrators of serious crimes; and an exchange of diplomatic notes memorializing the intent to report LASP data according to INTERPOL's standards. Pre-existing arrangements with some VWP countries that allow for the exchange of equivalent information are reviewed by an interagency working group and may be deemed sufficient in place of HSPD-6, the PCSC, or the LASP diplomatic note. The nine countries that were designated after the 9/11 Act came into force were required to meet the Act's information-sharing requirements in advance of VWP designation, as will any other countries designated in the future.

Progress to Date and Plans to Move Forward

Currently, our primary focus as it relates to the VWP is bringing the 27 pre-2008 VWP countries into compliance with the 9/11 Act information sharing requirements by 2012. To date, the Department—in cooperation with its partner agencies—has made substantial progress in this endeavor. For example:

- Almost all VWP countries have now concluded an exchange of diplomatic notes with the United States expressing their intent to report LASP data to the United States via INTERPOL or other acceptable mechanism. We are confident that we will be able to complete the exchange of diplomatic notes with the remaining VWP countries in the coming months.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00469 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.274

- PCSC Agreements—which establish the framework for a new method of law enforcement cooperation by providing each party electronic access to their fingerprint databases on a query (hit/no hit) basis—have been signed with 14 VWP countries: the Czech Republic, Estonia, Finland, Germany, Greece, Italy, Latvia, Lithuania, Hungary, Malta, Portugal, South Korea, Spain, and Slovakia. Negotiations to conclude additional PCSC Agreements are under way and DHS fully expects to sign several new agreements in the next few months. Given the sensitive nature of these discussions, I would be happy to provide any additional details in a follow-up closed session.

- Details regarding HSPD-6 Arrangements are classified. The State Department leads the diplomatic outreach and conducts negotiations together with the TSC, which is the implementing agency. The State Department and TSC have a standing offer to provide classified briefings to Members on HSPD-6 progress.

In an effort to bring each VWP country into compliance with the 9/11 Act's information sharing requirements, the U.S. government (USG), through a White House interagency policy committee, has developed and adopted a compliance strategy that ties completion of the 9/11 Act requirements to each country's biennial review of continuing VWP eligibility. While the dates of expected compliance vary depending on where each country falls in the review cycle, all countries are expected to be fully compliant by no later than June 2012. Last month, all VWP posts were instructed by the Department of State to demarche their host governments on the applicable compliance deadlines.

The interagency compliance strategy calls for a series of measures that, beginning six months prior to the date of expected compliance, may be taken by the USG to apply pressure on countries that resist entering into good faith negotiations to conclude these agreements. While DHS prefers to work with VWP countries so as to maintain their designation, we will not hesitate – in consultation with other relevant agencies – to implement corrective actions or other measures as necessary, including possible probation or termination.

Remaining Challenges

Despite our progress to date in reaching information-sharing agreements with the pre-2008 VWP countries, work remains to be done. DHS—in cooperation with the Departments of State and Justice—has invested considerable resources over the past two years in negotiating and concluding PCSC Agreements. The PCSC Agreement requires intensive face-to-face discussions with foreign governments to explain the Agreement in detail and address each country's concerns.

Signing a PCSC Agreement is only *one* important part of the process. Implementation of the 14 PCSC agreements that have been signed is legally and technologically complex. For example, most VWP countries require parliamentary ratification for the agreement to take effect. Technologically, a common IT architecture must be developed to allow the

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00470 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.275

United States and each of its participating foreign partners to query each other's fingerprint database automatically. The technical architecture now being developed for Germany will be replicated with other VWP countries. We estimate that the exchange of biometric data with Germany will begin this fall. DHS expects that process to proceed rapidly and has begun discussions on implementation with a number of countries.

III) Overstays

DHS has until now refrained from disclosing and using overstay rates to help determine VWP eligibility because precise rates could not be accurately calculated. However, our systems, particularly our collection and verification of biographic departure records for air travelers, have now improved to the point where we are increasingly confident in the reliability of the data. I am pleased to report that preliminary data strongly indicate that VWP travelers are not a significant source of overstays.

Using standard automated protocols to compare departure data with prior arrival records and immigration status changes, US-VISIT has calculated that in FY 2009, 31 out of 36 VWP countries had overstay rates that were well below the two percent disqualification rate threshold that may lead to a country being placed on probation. US-VISIT is conducting a manual review of overstay records from the five countries that, using automated protocols (but not manual verification), yielded an *apparent* overstay rate over two percent. Thus far, this in-depth manual review has been completed for two countries and revealed overstay rates below two percent.

Manual reviews of automated overstay records conducted by US-VISIT in the past have consistently shown that a significant percentage of the *apparent* overstays had in fact departed the United States within the authorized period of admission or had otherwise lawfully adjusted their status in the United States. We are conducting further manual reviews for other countries to reach a point where we are confident that our evaluation is valid. At that point we will likely be in a position to release overstay rates for each VWP country and to begin to use this data to inform VWP decisions.

IV) Future of the VWP

DHS believes that the current security and information-sharing requirements for VWP countries provide the USG with sufficient and timely information to prevent entry and, in the vast majority of cases, travel to the United States of individuals who would try to exploit the program to do our country harm. As noted above, our primary objective at this time is to complete the required information-sharing agreements with all the pre-2008 VWP countries as expeditiously as possible.
Given the security benefits of VWP to the United States and the program's important role in strengthening international partnerships and travel security standards, DHS would support a carefully managed expansion of the VWP to select countries that meet the statutory standards and are willing and able to enter into a close security relationship with the USG and, particularly, DHS.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00471 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.276

At present, most of the countries that have expressed an interest in VWP designation have visa refusal rates higher than three percent or other concerns that would have to be mitigated prior to designation. DHS and the Department of State continue to consult with trusted international partners to determine whether VWP designation is possible in the future. DHS and its partner agencies are also pursuing, as feasible, VWP-style information-sharing agreements with countries that are currently ineligible for the VWP but may qualify for the program within the next five years.

Because DHS has not yet notified Congress that a biometric air exit system is in place, any significant expansion of the VWP is unlikely at present. The 9/11 Act allows the Secretary of Homeland Security to waive the low nonimmigrant visa refusal rate requirement (less than three percent) for those countries with refusal rates between three and 10 percent who also meet other requirements. However, the waiver authority has been suspended because the Secretary did not notify Congress that a biometric air exit system was in place by June 30, 2009. This means that countries interested in joining the VWP must once again meet the less-than-3-percent refusal rate requirement until DHS implements a biometric air exit program.

As we know, no single security solution on its own will completely address the challenge of preventing *mala fide* individuals from traveling to the United States. Travel security systems of mutually reinforcing layers—involving such features as rigorous visa issuance standards, the use of visa security units, the screening of passengers through automated targeting systems, and forward-deployed border and immigration security officers—are critical in our efforts to thwart the travel of terrorists and other dangerous people. The VWP is of course a vital part of a robust travel security system for many reasons: the ESTA requirement; the mandatory bilateral information sharing arrangements regarding potential terrorists and criminals; sharing of LASP data; thorough inspections of VWP countries' transportation, aviation, border control, and travel document security standards; and vigorous, ongoing monitoring of changing conditions in VWP countries.

Chairman Lieberman, Senator Collins and other distinguished Members, thank you for the opportunity to appear before you today and for your consideration of this important topic. I would be happy to answer any questions that you might have.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00472 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.277

DEPARTMENT OF STATE

STATEMENT
OF

JANICE L. JACOBS

ASSISTANT SECRETARY OF STATE FOR CONSULAR AFFAIRS

BEFORE THE

SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING

ON

THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: SECURING THE VISA PROCESS

APRIL 21, 2010

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, thank you for the opportunity to address you today on the security of the visa process. As a result of the terrorist attack on Flight 253, the President ordered corrective steps to address systemic failures in procedures we use to protect the people of the United States. Secretary Clinton reiterated this direction when she stated, "we all are looking hard at what did happen in order to improve our procedures to avoid human errors, mistakes, oversights of any kind. We in the State Department are fully committed to accepting our responsibility for the mistakes that were made, and we're going to be working hard with the rest of the Administration to improve every aspect of our efforts." In the months following this attack, the Department of State has reviewed its Visas Viper reporting requirements as well as its visa issuance and revocation criteria, and introduced technological and procedural enhancements to facilitate and strengthen visa-related business processes.

Our immediate attention was on addressing the deficiencies identified following the attempted attack on Flight 253. In the case of Umar Farouk Abdulmutallab, on the day following his father's November 19 visit to the Embassy, we sent a cable to the Washington intelligence and law enforcement community through proper channels (the Visas Viper system) stating that "Information at post suggests [that Farouk] may be involved in Yemeni-based extremists." At the same time, the Consular Section entered Abdulmutallab into the Consular Lookout and Support System database known as CLASS. In sending the Visas Viper cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, but entered it correctly into CLASS. As a result of the misspelling in the cable, information about previous visas issued to him and the fact that he currently held a valid U.S. visa was not included in the cable. At the same time, the 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 Abdulmutallab was identified by DHS Customs and Border Protection (CBP) for secondary screening had the flight landed normally in Detroit. Additional reporting on

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00474 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.279

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 to call attention to the visa application and issuance material already present in the data that we share with our national security partners. In cabled instructions to the field, all officers were instructed to include complete information about all previous and current U.S. visa(s) in Visas Vipers cables. The guidance cable included specific instructions on methods to comprehensively and intensively search the database of visa records so that all pertinent information is obtained. I can confirm that these new requirements have been followed in all Visas Viper cables submitted since December.

In addition to these changes, we have reviewed the procedures and criteria used in the field to revoke visas and we are issuing new instructions to our officers. Revocation recommendations will be added as an element of reporting through the Visas Viper channel. In a March 22 cable to the field, we reiterated our guidance on use of the broad discretionary authority visa officers have 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.

The State Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, we have revoked 57,000 visas for a variety of reasons, including over 2,800 for suspected links to terrorism. We have been actively using this authority as we perform internal reviews of our data against updated watchlist information provided by partner agencies. For example, we are re-examining information in our CLASS database regarding individuals with potential connections to terrorist activity or support for such activity. We continue to review all previous Visas Viper submissions and cases that other agencies are bringing to our attention from the No Fly and Selectee lists, as well as other sources. In these reviews, we have identified cases

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00475 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.280

for revocation and confirmed that substantial numbers of individuals in these cases hold no visas, and of those few who did, a significant portion had visas that were revoked prior to the current review. We recognize the gravity of the threat we face and are working intensely with our colleagues from other agencies with the desired goal that no person who may pose a threat to our security holds a valid visa.

Revocation is an important tool in our border security arsenal. We will use revocation authority prior to interagency consultation in circumstances where we believe there is an immediate threat. At the same time, expeditious coordination with our national security partners is not to be underestimated. There have been numerous cases where our unilateral revocation without interagency coordination would have disrupted important investigations that were underway by one of our national security partners. They had the individual under investigation and our revocation action would have disclosed the U.S. Government's interest in the individual and ended our colleagues' ability to quietly pursue the case and identify terrorists' plans and co-conspirators.

Had these Visas Viper and revocation refinements been in place in Abuja on November 20, 2009, the actions taken by the officer, and the outcomes from those actions would have changed in the following ways:

- The consular officer would transmit a Visas Viper cable – as was done in the Abdulmutallab case – but, as mandated by our updated procedures, the officer would use our robust search engine to uncover Abdulmutallab's visa record in the database of visa records and report that information in the cable.

- The consular officer would enter a P3B (possible terrorist) entry into the Consular Lookout and Support System (CLASS, our automated repository of watchlist information) – as was done in the Abdulmutallab case.

- The Department would review the Visas Viper Cable upon receipt and, following expedited consultation with our interagency partners, revoke Mr. Abdulmutallab's visa, consistent with our post-12/26 policy that no one with a P3B entry holds a valid

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00476 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.281

visa. This revocation likely would occur on the day the Visas Viper cable is transmitted.

In addition to these changes in Visas Viper procedures, we immediately began working to refine the capability of our current systems. 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 27 million records found in CLASS. This strong search capability has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We are using this significant experience with search mechanisms for visa applications to improve the systems for checking our records of visas issued.

The Department of State has been 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 has evolved as post 9/11 reforms were instituted and is now performed by the Terrorist Screening Center (TSC). All records added to the Terrorist Screening Database are checked against the Department's Consular Consolidated Database (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 visa revocation. All such cases are carefully reviewed and most are revoked. Sometimes additional information is required from partner agencies. 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 DHS/Customs and Border Protection's (CBP) National Targeting Center (NTC) and other entities. 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 per day/7 days per week to address urgent requests, such as when the person is about to board a plane. In those circumstances, the State Department can use its authority to prudentially revoke the visa and prevent boarding.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00477 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.282

Since the Presidentially-ordered Security Review, individuals have been added to the Terrorist Screening Database, No Fly, and Selectee lists to counter the specific vulnerability observed on December 25, 2009. The number of revocations has increased substantially as a result. As soon as information is established to support a revocation, an entry showing the visa revocation is added electronically to the Department of State's lookout system and shared in real time with the DHS lookout systems used for border screening.

Consular officers refused over 2 million visas out of some 8 million applications in FY2009. No visa is ever issued without it being run through security checks against our partners' data, including screening applicants' fingerprints against U.S. databases as well.

Even as we instituted immediate measures, we planned for the future, incorporating new technology, increasing data sharing and enhancing operational cooperation with partner agencies. We have a record of quickly adapting and improving our procedures to respond to security imperatives. We have a highly trained global team working daily to protect our borders and fulfill the overseas border security mission and other critical tasks ranging from crisis management to protection of American interests abroad. Within the Department we have a dynamic partnership between the Bureau of Consular Affairs and the Bureau of Diplomatic Security, the Office of the Coordinator for Counter Terrorism, and the Bureau of Intelligence and Research that add valuable law enforcement and investigative component and intelligence analysis to our capabilities. We use these strengths to address the continuing security threats.

The Department has a close and productive partnership with DHS, which has authority for visa policy. Over the past seven years both agencies significantly increased resources, improved procedures, and upgraded systems devoted to supporting the visa function. DHS receives all of the information collected by the Department of State during the visa process. DHS has broad access to our entire CCD, containing 136 million records related to both immigrant and nonimmigrant visas and covering visa actions of the last 13 years. Special extracts of data are supplied to elements within DHS, including

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00478 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.283

the Visa Security Units (VSUs) of Immigration and Customs Enforcement (ICE). These extracts have been tailored to the specific requirements of those units.

We are working closely with ICE Visa Security Units (VSUs) established abroad and with domestic elements of DHS, such as CBP's National Targeting Center. Pursuant to an October 2004 Memorandum of Understanding between the Department of State and the U.S. Immigration and Customs Enforcement, Visa Security Unit (ICE/VSU) on the Administrative Aspects of Assigning Personnel Overseas, and National Security Decision Directive 38 (NSDD-38) we work collaboratively with DHS to determine where the establishment of a VSU is appropriate based on a number of factors, including the effectiveness of alternative arrangements for DHS staff, available space at the embassy, support capabilities, and security concerns.

VSUs currently operate at 14 visa adjudicating posts in 12 countries. Since January 19, 2010, we received requests from DHS's Immigration and Customs Enforcement to open four additional VSUs and to augment staff at two existing VSUs. The Chiefs of Mission at those respective posts approved the four new VSUs and one request for expansion; with one request for expansion pending. Later this year, a joint State Department (consisting of officers from the Bureaus of Consular Affairs and Diplomatic Security)-DHS team will visit more Foreign Service posts to consider the establishment of additional VSUs.

DHS has access to U.S. passport records, used by CBP to confirm the identity of citizens returning to the U.S. We developed new card-type travel documents that work with the automated systems CBP installed at the U.S. land borders. We are collecting more information electronically and earlier in the process. Expanded data collection done in advance of travel will give DHS and partner agencies richer information and more time for analysis.

We make all of our visa information available to other involved agencies, and we specifically designed our systems to facilitate comprehensive data sharing. Other

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00479 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.284

agencies have immediate access to over 13 years of visa data, and they use this access extensively. In November 2009, more than 16,000 employees of DHS, the Departments of Defense (DOD) and Commerce, and the FBI made 920,000 queries on visa records. We embrace a layered approach to border security screening and are fully supportive of the DHS Visa Security Program.

The Department of State is at the forefront of interagency cooperation and data sharing to improve border security, and we have embarked on initiatives that will position us to meet future challenges while taking into consideration our partner agencies and their specific needs and requirements. We are implementing a new generation of visa processing systems that will further integrate information gathered from domestic and overseas activities. We are restructuring our information technology architecture to accommodate the unprecedented scale of information we collect and to keep us agile and adaptable in an age of intensive and growing requirements for data and data sharing.

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 process on the globe. We were a pioneer in the use of facial recognition techniques and remain a leader in operational use of this technology. In 2009, we expanded use of facial recognition from a selected segment of visa applications to all visa applications. We now are 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.

The Department of State is an integral player on the border security team. We are the first line of defense. Our global presence, foreign policy mission, and personnel structure

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00480 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.285

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. While national security is paramount, the issuance and refusal of visas has a direct impact on foreign relations as well. Visa policy quickly can become a significant bilateral problem that harms U.S. interests if handled without consideration of foreign policy impacts. 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 those possibilities.

We developed and implemented intensive screening processes requiring personal interviews, employing analytic interview techniques, incorporating multiple biometric checks, all built around a sophisticated global information technology network. This frontline of border security has visa offices present in virtually every country of the world. They are staffed by highly trained and multi-lingual personnel of the Department of State. 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.

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, D.C. that works very closely with the Bureau of Diplomatic Security, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging applications and applicants who lack credibility, who present fraudulent documents, or who give us false information adds a valuable dimension to our visa process.

The Bureau of Diplomatic Security adds an important law enforcement element to the Department's visa procedures. There are now 75 Assistant Regional Security Officer Investigators assigned to 73 consular sections overseas specifically devoted to maintaining the integrity of the process. This year, the Bureau of Diplomatic Security

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00481 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.286

approved up to 48 additional investigator positions to work in consular sections overseas. They are complemented by officers working domestically on both visa and passport matters. These Diplomatic Security officers staff a unit within the Bureau of Consular Affairs that monitors overseas visa activities to detect risks and vulnerabilities. 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 we will continue to automate processes to reduce the possibility of human error. We fully recognize that we were not perfect in our reporting in connection with the attempted terrorist attack on Flight 253. We are working and will continue to work not only to address that mistake but to continually enhance our border security screening capabilities and the contributions we make to the interagency effort.

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.

We are facing an evolving threat. The tools we use to address this threat must be sophisticated and agile. 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 of State 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.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00482 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.287

U.S. Immigration and Customs Enforcement

STATEMENT

OF

JOHN MORTON

ASSISTANT SECRETARY

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

"THE LESSONS AND IMPLICATIONS OF THE CHRISTMAS DAY ATTACK: SECURING THE VISA PROCESS"

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

Wednesday, April 21, 2010 - 10:00 a.m.
342 Dirksen Senate Office Building

INTRODUCTION

Chairman Lieberman, Ranking Member Collins, distinguished Members of the Committee:

On behalf of Secretary Napolitano, thank you for the opportunity to discuss the international efforts of U.S. Immigration and Customs Enforcement (ICE) to protect national security and prevent terrorist attacks. Today, I plan to discuss the Visa Security Program (VSP) in the context of the 9/11 Commission's findings, which emphasized the importance of our immigration system more thoroughly vetting individuals entering our country and developing functional counterterrorism measures.

Within the Department of Homeland Security (DHS), ICE's VSP is one of a number of programs designed to protect the homeland and identify individuals who present a risk before they can harm the United States. The VSP places a DHS law enforcement officer (i.e., an ICE special agent) in a United States embassy to work collaboratively with Department of State (DOS) consular officers and Diplomatic Security Agents to secure the visa adjudication process. Before describing the VSP, our budget, the plans for expansion, and challenges of expanding, let me describe ICE's international efforts more generally.

ICE's Presence Overseas

ICE, as the second largest federal investigative agency, has a significant international footprint. ICE, through our Office of International Affairs (OIA), has 63 offices in 44 countries, staffed by more than 300 personnel. ICE personnel in these offices collaborate with foreign counterparts in joint efforts to disrupt and dismantle transnational criminal organizations engaged in money laundering, contraband smuggling, weapons proliferation, forced child labor,

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00484 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.289

human rights violations, intellectual property rights violations, child exploitation, and human smuggling and trafficking, and facilitate repatriation of individuals with final orders of deportation.

In fiscal year (FY) 2009, ICE opened offices in: Amman, Jordan; Brussels, Belgium; Cartagena, Colombia; Guayaquil, Ecuador; and Jakarta, Indonesia and continued to expand its coordination with U.S. military commands, specifically United States Southern Command (SOUTHCOM), United States African Command (AFRICOM), and United States European Command (EUCOM). In FY 2010, to increase our overseas presence and advance the efforts to investigate crimes that reach beyond our borders, ICE is proposing to open offices in Afghanistan, Israel, Vietnam, and Yemen.

ICE's OIA is responsible for administering and staffing the VSP.

The Visa Security Program

During the creation of DHS, Congress gave DHS some oversight responsibilities for the visa process. Specifically, Section 428 of the Homeland Security Act (HSA) of 2002 authorized the Secretary of Homeland Security to: administer and enforce the Immigration and Nationality Act (INA) and other laws relating to visas; refuse visas for individual applicants in accordance with law; assign DHS officers to diplomatic posts to perform visa security activities; initiate investigations of visa security-related matters; and provide advice and training to consular officers. In short, the HSA directed DHS to assist in the identification of national security threats to the visa security process.

The visa adjudication process is often the first opportunity our government has to assess whether a potential visitor or immigrant presents a threat to the United States. The United States

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00485 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.290

Government has long recognized the importance of this function to national security. DHS regards the visa process as an important part of the border security strategy, and VSP is one of several programs focused on minimizing global risks. The VSP relies on trained law enforcement agents to look at an applicant in greater depth and examine their social networks and business relationships with a goal of developing information previously unknown to the United States Government to assess whether individual applicants pose security threats to the United States. ICE agents assigned to Visa Security Units (VSU) are professional law enforcement agents who focus on selected applicants and any connection the applicants may have to terrorism.

In the context of the visa security process, they begin by reviewing documents submitted by applicants, and reviewing the results of automated checks (from the Consular Lookout and Support System (CLASS), and others). To conduct a thorough investigation, an ICE agent assigned to a VSU must have the ability to interview the applicant of concern and must be exposed to local information to understand whether the applicant's affiliations raise any particular flags. Each individual VSU, with input from DOS, develops a targeting plan, based on assessed conditions and threats. Depending on the nature of the concern that an applicant poses a threat, the ICE agent's investigation may be complex and in-depth, in some cases taking months to complete. Of course, not every investigation lasts months. ICE agents assigned to the VSP are experienced law enforcement agents who have spent years developing interview, interrogation, and other skills while investigating crimes in the United States.

DHS does not participate in all visa adjudication procedures; rather, DHS becomes a part of the process following initial screening of an applicant. As such, where VSU's are present,

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00486 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.291

DOS consular officers and ICE agents must establish effective and productive partnerships in order to enhance the security of the visa process.

VSP efforts complement the consular officers' responsibility for interviewing the applicant, reviewing the application, and supporting documentation and conducting automated screening of criminal and terrorist databases, with proactive law enforcement vetting and investigation. In carrying out this mission, ICE special agents conduct targeted, in-depth law enforcement-focused reviews of individual visa applications and applicants prior to issuance, as well as recommend refusal or revocation of applications when warranted.

ICE now has VSU's at 14 high-risk visa adjudication posts in 12 countries. While I can not identify the specific posts in this forum, I will gladly brief the members and staff of this committee in a classified or law enforcement sensitive setting at a later date. At these 14 posts, in FY 2009, ICE agents screened 904,620 visa applicants and with their DOS colleagues determined that 301,700 required further review. Following investigation, in collaboration with their DOS colleagues, ICE recommended refusal of over 1,000 applicants. In every instance, DOS followed the VSU recommendation and ultimately refused to issue the visa. VSP recommendations have also resulted in DOS visa revocations.

Expansion of the Visa Security Program

Under the direction of the Homeland Security Council, beginning in May 2008, ICE and DOS collaborated on the development of the VSP Site Selection Methodology. In brief, the process for selecting a particular site for a VSU begins with an ICE site evaluation, which involves a quantitative analysis of threats posed and site assessment visits. The DHS formal nomination process follows, involving an analysis of ICE's proposals by DHS. Then, the

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00487 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.292

National Security Decision Directive-38 (NSDD-38) process, a mechanism that gives the Chief of Mission in a particular post control over the size, composition, and mandate of full-time staffing for the post, commences within DOS. Only once the Chief of Mission has approved an NSDD-38 request can ICE begin deployment.

ICE continues to look for opportunities to establish offices overseas to screen and vet additional visa applicants at high-risk visa issuing posts beyond the 14 posts at which we are currently operating. The FY 2010 budget designated $7.3 million to sustain and expand the VSP. With this funding level, ICE estimates that it can deploy to four additional posts. ICE has been conducting site visits and facilitating the NSDD-38 process in an effort to determine whether it would be beneficial to expand VSP operations to additional high-risk visa adjudicating posts. Based on collaborative site selection methodology with DOS, ICE conducted additional classified threat assessments on four posts in preparation for joint VSP-DOS site visits to embassies/consulates abroad. The VSP program has continued to grow since its inception. While ICE is continuing to expand the program, further expansion is contingent on ICE's dedicating existing overseas funding to these efforts and approval of NSDD-38 requests at the posts in question.

ICE will continue moving forward to deploy new offices to the highest risk visa adjudicating posts worldwide as resources allow, and will continue to conduct joint site visits with DOS to create opportunities for deployment. Moreover, ICE recognizes that the VSP is but one relatively small component in the nation's counterterrorism strategy. My counterparts at DOS and I are engaged now in a process of determining a common strategic approach to the broader question of how best to collectively secure the visa issuance process. We look forward to continuing to report back to you with updates on this process.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00488 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.293

Recent Successes

To put the VSP discussion in perspective, I offer two brief examples of the results of including ICE in the visa process. In September 2008, DOS raised concerns about visa applicants sponsored by an international non-governmental sports group. ICE investigated and determined that the majority of past applicants sponsored by the group remained in the United States beyond their period of admission, and that the sport group's president had three previous visa denials, with one on national security grounds. ICE disseminated information about potential future applicants throughout DHS and to DOS visa-issuing posts. This equipped CBP Inspectors stationed at airports and the border and DOS consular officers with detailed information about the sports group to prevent future use of the club as a mechanism to gain entry into the United States, and to prevent national security threats from exploiting the scheme to gain entry.

Secondly, in July 2009, again while examining visa applications, ICE agents identified an Iranian national who applied for a visitor's visa to come to the United States to attend an information technology (IT) conference on behalf of his employer. Although the Security Advisory Opinion (SAO) process did not reveal a basis to find the Iranian national ineligible, ICE's review revealed that the Iranian national's employer—on whose behalf he was attending the IT conference—is an Office of Foreign Assets Control (OFAC)-designated organization allegedly used by the government of Iran to transfer money to terrorist organizations, including Hezbollah, Hamas, the Popular Front for the Liberation of Palestine-General Command and Palestinian Islamic Jihad.

The visa applicant himself stated that he planned to attend the IT conference to explore the purchase of technology for his employer. While attending the conference alone did not

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00489 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.294

render the Iranian national inadmissible, the combination of attending on behalf of his employer (an OFAC-designated entity) and the stated purpose to "explore purchasing options" for IT equipment constituted reasonable grounds for denial of the visa. Therefore, ICE recommended that DOS deny the visa on national security grounds, in accordance with the INA, as his purpose for coming to the United States was to possibly procure IT equipment for a designated OFAC organization. DOS concurred with ICE's recommendation and denied the visa.

I offer these examples to illustrate in real terms the benefit of a strong working relationship with DOS, and how the partnership advances the goal of preventing those who may intend to harm the United States from using a visa to enter our nation.

The Visa Security Program's Security Advisory Opinion Unit (SAOU)

The Security Advisory Opinion (SAO) process is the mechanism administered by DOS, supported by other government agencies, to provide consular officers advice and background information to adjudicate visa applications abroad in cases of security or foreign policy interest. In May 2007, Congress mandated the creation of a Security Advisory Opinion Unit (SAOU) within the VSP. VSP now supports the SAO process and the SAOU's findings are incorporated into the overall SAO recommendation used by consular officers to adjudicate targeted visa applications of national security or foreign policy interest.

The SAOU is currently operating a pilot program that screens visa applicants and communicates any potential admissibility concerns to DOS. The SAOU currently has co-located personnel at the Human Smuggling and Trafficking Center (HSTC), the National Targeting Center-Passenger (NTC-P), both located in the National Capital Region, and also has personnel assigned to the National Counterterrorism Center (NCTC). The integration of the SAOU into

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00490 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.295

these centers allows for real-time dissemination of intelligence between the various stakeholders in the visa adjudication process.

CONCLUSION

I would like to thank the Committee for the opportunity to testify today and for its continued support of ICE and our law enforcement mission. In partnership with the State Department and other vital partners, I will continue collaborating to ensure the security of the visa while maintaining a fair and efficient process for legitimate visitors and immigrants to enter the United States.

I would be pleased to answer questions you may have at this time.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00491 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.296

Post-Hearing Questions for the Record
Submitted to the Honorable David F. Heyman and the Honorable John T. Morton
From Senator Joseph I. Lieberman

"The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process"
April 21, 2010

Question#:	1
Topic:	expansion
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In the eight years since the creation of the Visa Security Program, only 14 of the more than 200 consular posts that issue visas have received Visa Security Units. A joint DHS-State study resulted in a plan for implementing the program at all 57 high risk consular posts by 2013. Given the slow pace of implementation, and the fact that the FY2011 budget does not include any new funding for continuing to expand the program, this no longer seems likely.

When do you believe that the Visa Security Program will be deployed to all of the 57 high-risk posts identified by the joint DHS-State review?

Response: The U.S. Immigration and Customs Enforcement (ICE) Visa Security Program (VSP) has continued to expand since its inception. Future expansion and the rate of expansion are dictated by several factors. Additionally, beginning in May 2008 and under the direction of the Homeland Security Council, ICE and DOS collaborated on the development of the VSP Site Selection Methodology. The process for selecting a particular site for a Visa Security Unit (VSU) begins with an ICE site evaluation, which involves site assessment visits and a quantitative analysis of potential threats. The DHS formal nomination process follows, involving a DHS analysis of ICE's proposals. Then, DOS commences the standard National Security Decision Directive-38 (NSDD-38) process, a mechanism that gives the Chief of Mission, as the President's representative, control over the size, composition, and mandate of full-time mission staffing for all U.S. Government agencies. Once the Chief of Mission has approved an NSDD-38 request, ICE can begin deployment. ICE continues to look for appropriate posts at which to establish VSUs. ICE has been conducting site visits and facilitating the NSDD-38 process in an effort to expand VSP operations to additional high-risk visa adjudicating posts beyond the 14 posts at which ICE VSP is currently operating.

56838.297

Question#:	1
Topic:	expansion
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: What are the main reasons for the slow pace of expansion?

Response: ICE has deployed consistent with available resources; in addition, although ICE may identify a possible site for deployment, as with any other overseas office, it is necessary that the Chief of Mission at that site approve the request.

While ICE's cooperation with COM's has been largely successful, each request represents an individual negotiation with a particular embassy based, for example, on the location's particular space and resource constraints as well as prevailing security concerns. ICE continues to coordinate site selections and visits to posts under consideration for ICE deployment in order to consult with the Chiefs of Mission.

56838.298

Question#:	2
Topic:	strategic plan
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In 2005, GAO reviewed the Visa Security Program and concluded that "DHS has not developed a strategic plan outlining the Visa Security Program's mission, activities, program goals, and intended results for operations." GAO also faulted DHS for not keeping track of important performance measures related to the Visa Security Program. In 2008, the DHS OIG noted that ICE needed to enhance the "recording, tracking, monitoring, verification, analysis, and reporting of visa security activities."

Does ICE or DHS have a strategic plan in place today that addresses the programs' mission, activities, goals, and intended results? If so, please share it with the Committee. If not, please explain why not and when such a plan will be put in place.

Response: Since the 2005 GAO report, ICE developed the Visa Security Program (VSP) Expansion Plan in February 2007, which serves as a strategic framework for the VSP and outlines expected expansion plans for the next five years, including preliminary budget projections. (Per your request, a copy is enclosed.) The ICE Assistant Secretary, Department of Homeland Security (DHS), the Homeland Security Council, and the Office of Management and Budget (OMB) approved the plan in 2007. In addition, the National Strategy for Homeland Security, issued in October 2007, includes expanding law enforcement personnel overseas whose role would be to focus on assessing national security threats and fraudulent documents used in the visa application process. VSP expansion is also supported in the National Counterterrorism Center's (NCTC) National Implementation Plan for The War on Terror.

Question: Does ICE collect performance measures and data on the reasons why Visa Security Units have recommended that consular officers deny visas? In other words, for terrorism-related reasons versus concerns about an intending immigrant? If so, please provide the Committee with a detailed analysis of the reasons for visa denial recommendations made by VSP officers, broken down by post and by year.

Response: In February 2010, ICE began implementing a robust set of performance measures to demonstrate the VSP's impact. Monthly reports that track over 65 measures, two of which are Government Performance and Results Act of 1993 (GPRA) metrics, identify the number of instances in which an ICE special agent recommended refusal of a visa application, resulting in a consular officer's decision to deny a visa. As noted in the 2008 Office of the Inspector General (OIG) report on the VSP, ICE's previous VSP case

56838.299

Question#:	2
Topic:	strategic plan
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

management system had a number of limitations. This deficiency has since been corrected by the development of a new case management system. In conjunction with the Department of State (DOS), ICE developed an updated system which is a web-based, globally accessible system that will provide the necessary analytical, reporting, and data storage capabilities the program requires. Deployment of this system began in February 2010 and will be complete in the summer of 2010.

In light of the challenges that Visa Security Units faced due to the limitations of the legacy VSP tracking system, the process to obtain the number of visa denials by officers by reason broken down by post is impractical and would yield unreliable results. The newly deployed case management system has addressed this shortcoming and these numbers will be available going forward, but the statistics are not available retroactively. "Recommended Refusals" by post are included below.

By mutual agreement with DOS, VSP officers deployed abroad do not recommend refusals to DOS based on § 214(b) of the Immigration and Nationality Act (INA), which addresses intending immigrants. Such adjudications are made by individual consular officers adjudicating cases at post. VSP officers routinely provide information to consular officers that relates to intending immigrants and INA § 214(b) and consular officers may make § 214(b) determinations based on information provided by VSP officers. VSP refusal recommendations may include other sections of the INA except for § 214(b).

VSP RECOMMENDED REFUSALS TO DOS BY POST FY 2007 – 2009

POST	FY 07 TOTAL	FY 08 TOTAL	FY 09 TOTAL
Abu Dhabi	**95**	**122**	**238**
Amman	**0**	**0**	**5**
Cairo	**262**	**236**	**24**
Caracas	**16**	**49**	**53**
Casablanca	**0**	**3**	**98**
Dhahran	**2**	**2**	**0**
Dubai	**35**	**100**	**159**
Frankfurt	**0**	**0**	**60**
Hong Kong	**5**	**14**	**5**
Islamabad	**5**	**19**	**68**

56838.300

Question#:	2
Topic:	strategic plan
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Jakarta	**0**	**0**	**14**
Jeddah	**0**	**0**	**0**
Manila	**283**	**299**	**153**
Montreal	**14**	**14**	**109**
Riyadh	**39**	**37**	**33**
Totals	**756**	**895**	**1027**

Question: Does DHS believe that it needs enhanced authorities to be a more effective partner with State in the Visa Security Program? What specific authorities do you believe are needed?

Response: DHS has a close cooperative relationship with the Department of State. At this time, DHS has not identified the need for enhanced authorities relating to the Visa Security Program.

56838.301

Question#:	3
Topic:	ESTA
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The 9/11 Commission noted that every interface with a government official is an opportunity to catch a terrorist, and the visa waiver program eliminates a number of steps that most travelers to the United States have to go through. In order to address this, this Committee implemented a number of changes to the program including requiring enhanced information sharing and the creation of the Electronic System for Travel Authorization.

The Committee is concerned about the number of visa waiver nations that have yet to sign agreements with the United States to share biometric criminal information and terrorist watchlist information. Can you describe for the Committee what the obstacles are to continuing to expand these agreements?

The Committee is even more concerned that, although in the past few years we have signed agreements with some 15 nations to date, we have yet to actually implement even one of these agreements. This means that we are not actually sharing the information we have agreed to share—at least not electronically. Can you explain to the Committee why these agreements have yet to be actually implemented? Does DHS have a timeline for implementing these agreements? If not, what steps is DHS taking to ensure that these agreements are implemented in an expedited manner.

Response: The "*Implementing Recommendations of the 9/11 Commission Act of 2007*" (9/11 Act) requires that Visa Waiver Program (VWP) countries enter into an agreement with the United States to share information regarding whether citizens and nationals of the country represent a threat to the security or welfare of the United States and its citizens. The Department of Homeland Security (DHS), with the support of interagency partners, has determined that the preferred mechanisms to meet the information sharing requirements include a bilateral Homeland Security Presidential Directive-6 (HSPD-6) Arrangement to exchange terrorism screening information and a bilateral Preventing and Combating Serious Crime (PCSC) Agreement to exchange information on possible perpetrators of serious crimes. Details regarding HSPD-6 Arrangements are classified. The State Department leads the diplomatic outreach on HSPD-6 and conducts negotiations together with the Terrorist Screening Center (TSC), which is the implementing agency for the Arrangement. The State Department and TSC have made a standing offer to conduct a classified briefing for Members and staff on the HSPD-6 program.

56838.302

Question#:	3
Topic:	ESTA
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

DHS and the Department of Justice (DOJ) have the lead for negotiating PCSC Agreements. Concluding these agreements usually involves a lengthy process that presents several inherent challenges. For example, in most cases, finalizing a PCSC Agreement requires intensive, face-to-face discussions in order to: explain the Agreement in detail and highlight the unique benefits it offers; address concerns raised by the foreign government (usually involving data privacy and redress procedures for the country's citizens); ensure that requested changes to the Agreement adhere to U.S. laws and policies; and answer other complex legal and technical questions, among other issues. Negotiations can also be time-consuming because they normally require the participation and final approval of two to three different foreign government ministries. Moreover, concluding a PCSC Agreement can be politically sensitive for foreign governments, as final approval often requires parliamentary ratification. The ratification process often entails the public release of the Agreement.

In an effort to bring each VWP country into compliance with the 9/11 Act's information sharing requirements, the U.S. government (USG), through a White House interagency policy committee, has developed and adopted a compliance strategy that ties completion of the 9/11 Act requirements to each country's biennial review of continuing VWP eligibility. The interagency compliance strategy calls for a series of measures that, beginning six months prior to the date of expected compliance, may be taken by the USG to apply pressure on countries that resist entering into good faith negotiations to conclude information sharing agreements. While the dates of expected compliance vary depending on where each country falls in the review cycle, all countries are expected to be fully compliant by no later than June 2012. DHS prefers to work with VWP countries so as to maintain their designation, but is prepared – in consultation with other relevant agencies – to implement corrective actions or other measures as necessary, including possible termination.

Implementation of the PCSC Agreements that have been signed is legally and technically complex. Most VWP countries require parliamentary ratification for the agreement to take effect. Technologically, a common Information Technology (IT) architecture must be developed to allow the United States and each of its participating foreign partners to query each other's fingerprint database automatically. DHS and the DOJ are currently establishing the common technical architecture with Germany and DHS estimates that the exchange of biometric data with Germany will begin this fall. DHS assesses that once the common technical architecture has been established, it will allow the Department to proceed rapidly on implementation discussions with other countries. DHS has already begun preliminary discussions on implementation with a number of countries, including the Republic of Korea and Hungary.

56838.303

Post-Hearing Questions for the Record
Submitted to the Honorable David F. Heyman and the Honorable John T. Morton
From Senator Claire McCaskill

"The Lessons and Implications of the Christmas Day Attack:
Securing the Visa Process"
April 21, 2010

Question#:	4
Topic:	air exit
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The Visa Waiver Program is currently limited to an extent by the success and roll-out of the air exit system. For example, without an air exit system, the Secretary for the Department of Homeland Security (DHS) cannot provide a waiver to those countries that do not meet the 3% minimum requirement for a nonimmigrant visa refusal rate. I understand that there are two pilots that are being conducted.

What is the status of these pilot programs?

Response: Congress included a provision in the *Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009* (Public Law 110-329) requiring DHS to test and provide a report assessing specific options with respect to collection of biometrics from most non-U.S. citizens exiting the United States prior to spending funds to implement the "final air exit solution" described in the notice of proposed rulemaking at 73 Fed. Reg. 22065 (Apr. 24, 2008) (US-VISIT Exit NPRM).

Though no airline agreed to participate in a pilot, DHS completed pilots in two different settings at airports where passengers are already subject to the United States Visitor and Immigrant Status Indicator Technology Program's (US-VISIT) entry requirements. Both pilots began on May 28, 2009 and concluded on July 2, 2009. The results of these pilots are contained in a report submitted to the House and Senate Committees on Appropriations, Subcommittees on Homeland Security on October 26, 2009.

Sections 217(c)(8) and (i) of the Immigration and Nationality Act (INA) set forth biometric air exit requirements specific to the Visa Waiver Program. Under section 217(c)(8), the Secretary of Homeland Security may waive the low nonimmigrant visa refusal rate requirement for designation as a program country if certain conditions are

56838.304

Question#:	4
Topic:	air exit
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

met. That authority came into effect in 2008 upon certification by the Secretary that an air exit system was in place that could verify the departure of not less than 97 percent of foreign nationals who exit through airports of the United States. The waiver authority was suspended when the Secretary was unable to notify Congress that the air exit system met the biometric requirements in section 217(i) by June 30, 2009.

DHS is examining the results of the US-VISIT Exit pilots required by Public Law 110-329 and other related pilots and considering options for a path forward with regard to collection of data of non-U.S. citizens exiting the United States. As part of that analysis, DHS will evaluate the impact of such decision making on the safety and security of the United States, cost-related concerns, as well as other considerations, such as the authority of the Secretary to waive the low nonimmigrant visa refusal rate requirement to designate additional Visa Waiver Program (VWP) countries.

Question: What is the roll-out plan for the air exit system and what are the associated costs?

Response: DHS has performed significant planning and testing over the last several years examining possible solutions for integrating biometric exit requirements into the international air departure process. Detailed descriptions of the options and costs are included in an economic analysis to accompany DHS' proposed rule for biometric exit published in the Federal Register on April 24, 2008 at 73 FR 22065. In short, however, DHS has examined a variety of collection agents (whether government or commercial carrier) and locations (whether airline gate, TSA checkpoint, or airline check-in counter). Depending on the option chosen, the estimated costs are between $3 and $9 billion over a ten year period.

Question: Are these costs included in the FY11 President's Budget?

Response: Cost effectiveness and efficiencies are among the critical factors that will contribute to the decisions we make on implementing a new biometric air exit program. DHS has not made any decisions at this time and is still examining options for biometric exit to include all comments received from the proposed rule and the results of the 2009 exit pilots. DHS will not submit appropriations requests until we are certain that we have identified a viable path forward for implementing biometric exit in the air, sea, and land environments. Future funding requests for biometric exit will be produced during the formal administration budgeting cycle as appropriate.

Question: What is the contingency plan if the air exit system is not feasible or affordable?

Response: DHS is currently examining options in order to meet the statutory requirement to create a biometric exit program. DHS will continue to keep Congress informed of all developments in its analysis.

56838.305

Question#:	5
Topic:	MOU
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: On September 28, 2003, then-Secretary of State Colin Powell and then-Secretary of Homeland Security Thomas Ridge signed the memorandum of understanding (MOU) implementing §428 of the Homeland Security Act of 2002. The MOU described each department's responsibilities in the area of visa issuances. Among its major elements, the MOU stated that the Department of State (DOS) may propose and issue visa regulations subject to Department of Homeland Security (DHS) consultation and final approval.

How many of these major visa regulations have been approved since 2003? What were they?

Has DHS and DOS had any disagreements over any of the regulations? What was the outcome?

Response: Section 428 (b) of the Homeland Security Act of 2002 (HSA) (6 U.S.C. 236 (b)) provides that the Secretary of Homeland Security is "vested exclusively with all authorities to issue regulations with respect to, administer, and enforce the provisions of [the Immigration and Nationality Act], and of all other immigration and nationality laws, relating to the functions of consular officers of the United States in connection with the granting or refusal of visas…." Under paragraph 2 of the Memorandum of Understanding Between the Secretaries of State and Homeland Security Concerning Implementation of Section 428 of the Homeland Security Act of 2002 (MOU), the Department of State may propose and issue visa guidance subject to DHS consultation and final approval, except in those areas that are the specific responsibility of the Secretary of State as set forth in the HSA or other applicable authorities as specified in the MOU.

Since 2003, the Department of State has published 184 visa-related regulations and notices requiring DHS consultation and final approval. These regulations are included as an attachment.

The DOS consults with DHS both directly and through the Office of Management and Budget's interagency review process when promulgating visa-related regulations. In this manner, DHS is afforded the opportunity to comment, and DOS responds to DHS's concerns.

56838.306

List of Published Regulations from 2003 until today from Directives Management in 22 CFR

For 2003:

- Final Rule 22 CFR Part 9 National Security Information Regulations 4/7/2003

- Proposed Rule 22 CFR 96 Hague Convention on Intercountry Adoption; Intercountry Adoption Act of 2000 9/2/2003

- A-RPS-IPS proposed rule 22 CFR 171 Availability of Info to Public 4/2/2003

- A-RPS-IPS proposed rule 22 CFR 9 National Security Information 4/7/2003

- CA-OCS-PRI direct final rule 22 CFR 32 Stolen Vehicles - Mexico 5/12/2003

- CA-VO final rule 22 CFR 41.24 DOCUMENTATION OF NONIMMIGRANTS UNDER THE IMMIGRATION AND NATIONALITY ACT, AS AMENDED - ADDITIONAL INTERNATIONAL ORGANIZATION 5/23/2003

- CA-VO final rule 22 CFR 41.107(c)(1) visa fee waivers for UN observer missions 3/7/2003

- CA-VO final rule 22 CFR 42.21 Documentation of Immigrants Under the Immigration and Nationality Act, as Amended – Immediate Relatives Immediate Relatives 3/7/2003

- CA-VO final rule 22 CFR 42.72(e) Elimination of Extended Visa Benefits 3/14/2003

56838.318

- CA-VO final rule 22 CFR 42.74(b) Replacement Visas 3/7/2003

- CA-VO-L-R final rule 22 CFR 41 Suspension of Transit Without Visa Program 3/7/2003

- CA-VO-L-R final rule 22 CFR 41.12 Visa Categories 3/7/2003

- CA-VO-L-R final rule 22 CFR 41.112(d) Automatic Visa Revalidation 8/11/2003

- CA-VO-L-R interim rule 22 CFR 41.64T Documentation of Nonimmigrants Under the Immigration and Nationality Act, as Amended -- Victims of Severe Forms of Trafficking in Persons 6/19/2003

- CA-VO-L-R interim rule 22 CFR 41.102 Documentation of Nonimmigrants Under the Immigration and Nationality Act, As Amended; Personal Appearance 6/18/2003

- CA-VO-L-R interim rule 22 CFR 41.102 Personal Appearance Waiver 6/18/2003

- CA-VO-L-R interim rule Electronic Diversity Visa Petition 8/12/2003

- EB-TRA final rule 22 CFR 89 Foreign Prohibitions on US Longshoremen Work 12/2/2003

- PM-DDTC final rule 22 CFR 126 ITAR 12/11/2003

- PM-DTC final rule 22 CFR 126 AES ITAR 10/9/2003

56838.319

- PM-DTC final rule 22 CFR 120 ITAR DDTC Realignment 9/29/2003

- PM-DTC final rule 22 CFR 120 ITAR DTC Reorganization 1/31/2003

- CA Final Rule 22 CFR 41.12 Visas Documentation of Nonimmigrants Under the Immigration and Nationality Act 8/5/2003

- Final Rule 22 CFR Part 9 National Security Information Regulations 4/7/2003

- Proposed Rule 22 CFR 96 Hague Convention on Intercountry Adoption; Intercountry Adoption Act of 2000 9/2/2003

For 2004

- A-OPE Proposed Rule 48 CFR Parts 619, 625, 628, and 652 DOSAR 12/1/2004

- A-RPS-IPS final rule 1400-AB85 22 CFR 171 Availability of Information to the Public 10/13/2004

- CA-EX final rule 22 CFR 22 CA-EX final rule 1400-AB94 entire with table 9/1/2004

- CA-EX Interim Rule 22 CFR 22 Schedule of Fees for Consular Services; Exemption from the Nonimmigrant Visa Application Processing Fee for Family Members of Individuals Killed or Critically Injured While Serving the United States 8/18/2004
- CA-PPT interim rule 22 CFR 51 Passport Procedures—Amendment to Passport Regulations 2/18/2004

- CA-PPT interim rule 22 CFR 51 Both Parent Passport Approval 10/6/2004

- CA-PPT proposed rule 22 CFR 51 Electronic passport 12/13/2004

56838.320

- CA-VO final rule 22 CFR 22 Schedule of Fees for Consular Services, Department of State and Overseas Embassies and Consulates 12/15/2004

- CA-VO-L-R interim final rule 22 CFR 41.42 Crew List Visa Elimination 1/16/2004

- ECA-EC-AG Final Rule 22 CFR 62 Participation in the Exchange Visitor Program as Professor and Research Scholar 12/17/2004

- G-TIP Final Rule 22 CFR 96 International Trafficking in Persons : Interagency Sharing of Information and Coordination of Activities 11/23

- PM-DDTC Interim Rule 22 CFR Parts 122 and 129 ITAR Fee Change 11/23

- PM-DTC Final Rule 22 CFR 126 Amendment to the International Traffic in Arms Regulations 2/11

- PM-DTC Final Rule - 22 CFR Parts 121 and 123 Amendment to the International Traffic in Arms Regulations: United States Munitions List 3/30/2004

- PM-DTC Interim Rule 22 CFR Parts 122 and 129 Amendment to the International Traffic in Arms Regulations: Registration Fee Change 12/3

For 2005

- A-OPE final rule 48 CFR Parts 601, 611, 619, 622, 628, and 652 DOSAR 11/29/2005

- CA VO Final rule 22 CFR nomenclature changes INS-DHS 3/24

56838.321

- CA-EX final rule 22 CFR 98 Intercountry Adoption—Preservation of Convention Records 8/19

- CA-OCS final rule 22 CFR 98 Intercountry Adoption 8/19

- CA-PPT proposed rule 22 CFR 51 Electronic Passport 2/11

- CA-PPT final rule 22 CFR 51 Electronic Passport 10/25

- CA-PPT final rule 22 CFR 51 New Passport Amendment Policy 9/8

- CA-VO-L-R final rule 22 CFR 41 Visas: Treaty trader, Treaty investor, or Treaty alien in a specialty occupation 6/29

- CA-VO-L-R final rule 22 CFR 41 Documentation of Nonimmigrants Under the Immigration and Nationality Act, as Amended—Student and Exchange Visitor Information System (SEVIS) 2/10

- CA-VO-L-R final rule 22 CFR 41 Documentation of Nonimmigrants Under the Immigration and Nationality Act, as Amended—Irish Peace Process Cultural and Training Program, Q Classification 10/6

- CA-VO-L-R interim rule 22 CFR 40 Aliens Inadmissible Under the Immigration and Nationality Act—Unlawful Voters 6/14

- CA-VO-L-R final rule 22 CFR Chapter I Nomenclature Change Reflecting Department of Homeland Security 3/28

- CA-VO-L-R proposed rule 22 CFR 41 Documentation of Nonimmigrants Under the Immigration and Nationality Act, as Amended—Air Transit Program 5/9

56838.322

- CA-VO-L-R proposed rule 22 CFR 42 Hague Convention on Intercountry Adoption Act of 2000; Consular Officer Procedures in Convention Cases 12/16

- Ca-VO-L-R 22 CFR 40 Aliens Inadmissible Under the Immigration and Nationality Act—Unlawful Voters 5/13

- ECA final rule 22 CFR Part 62 Participation in the Exchange Visitor Program as Professor and Research Scholar 5/13

- ECA-EC-AG final rule 22 CFR 62 Research Scholar 2/8

- G-TIP final rule 22 CFR 96 International Trafficking in Persons: Interagency Sharing of Information and Coordination of Activities 9/30

- L-EMP final rule 1400-AC09 Removal of 22 CFR Part 10 11/3

- PM-DTC final rule 22 CFR Parts 122, 129 Amendment to the International Traffic in Arms Regulations: Registration Fee Change 10/7

- PM-DTC final rule 22 CFR 126 ITAR amendments 7/6

- PM-DTC final rule 22 CFR 126 Amendment to the International Traffic in Arms Regulations: Section 126.1(i) 8/23

- PM-DTC final rule 22 CFR Parts 120, 123, 124, 126, 127 Amendment to the International Traffic in Arms Regulations: Port Directors Definition, NATO Definition, Major Non-NATO Ally Definition, Recordkeeping Requirements, Supporting Documentation for Electronic License Applications, 8/22

56838.323

- RM final rule 22 CFR Part 17 Overpayments From the Foreign Service Retirement and Disability Fund 12/29

- RM final rule 22 CFR 34 Debt Collection 12/29

For 2006

- A-ISS-IPS-IP Proposed Rule 22 CFR Part 9 National Security Information Regulations 1/09/2006

- A-ISS-IPS-IP Proposed Rule 22 CFR Part 171 Search Fees in Freedom of Information Act Cases 10/20

- A-OPE Final Rule 48 CFR Parts 601, 611, 619, 622, 628, and 652 Department Of State Acquisition Regulations 6/13
- A-OPE Final Proposed 48 CFR Part 601 Department Of State Acquisition Regulations 12/15

- CA-EX Interim Final 22 CFR Part 51 Passport Procedures-Amendment to Passport Regulations 5/19

- CA-EX FINAL 22 CFR Part 51 Passport Procedures-Amendment to Restriction of Passports Regulation 9/29

- CA-OCS Final 22 CFR Part 96 Intercountry Adoption Implementation 2006-01-09

- CA-OCS-CI Final Rule 22 CFR Part 99 Intercountry Adoption Reporting on Non-convention and Convention Adoptions of Immigrating Children 6/23

56838.324

- CA-OCS-PRI Final Rule 22 CFR Part 97 Intercountry Adoption Certificates 10/27

- CA-OCS-PRI Final Rule 22 CFR Part 42 Hague Convention on Intercountry Adoption 05/26

- CA-OCS-PRI Proposed Rule 22 CFR Part 51 Passport Regulations 10/230

- CA-OCS-PRI Proposed Rule 22 CFR Part 72 Overseas Death and Estate Procedures 10/19

- CA-PPT-PAS Proposed Rule 22 CFR Parts 22 & 51 Card Format Passport Changes to Passport Fee Schedule 10/11

- CA-VO-L-R Final Rule 22 CFR Part 41 Documentation of Nonimmigrants under the Immigration and Nationality Act 8/21

- CA-VO-L-R Final Rule 22 CFR Part 41 Documentation of Nonimmigrants Under-Irish Peace Process 5/2

- CA-VO-L-R Final Rule CFR Part 41 Documentation of Nonimigrants-Waiver of Personal Appearance 12/13

- CA-VO-L-R Final Rule 22 CFR Parts 40, 41, and 42 Nomenclature Changes Reflecting Creation of Department of Homeland Security 6/5

- CA-VO-L-R Interim Rule 22 CFR Part 40 Aliens Inadmissible Under the Immigration and Nationality Act—Traffickers in Persons 1/9

- CA-VO-L-R Proposed Rule CFR 22 Part 40 Hague Convention on Intercountry Adoption 06/13

56838.325

- ECA-EC Final Rule 22 CFR Part 62 Au Pair Exchange Programs 6/1

- ECA-EC Final Rule 22 CFR Part 62 Secondary School Student Exchange Program 3/27

- ECA-EC-PS Proposed Rule 22 CFR Part 62 Exchange Visitor Program Training and Internship Program 3/31

- VO- Final Rule 22 CFR 41 Documentation of Nonimigrants-Waiver of Personal Appearance 11/2

- G-TIP Final Rule CFR Part 96 TIP Interagency Sharing Move 03/02

- L-T Proposed Rule 22 CFR Part 181 Publication Coordination and Reporting of International Agreements-Amendments 05/11

- L-T Final Rule 22CFR 181 Publication, Coordination, and Reporting of International Agreements-Amendments 09/01

- PM-DTCC Final Rule 22 CFR 122 & 129 Registration Fee Change 01/13

- PM-DTCC Final Rule 22 CFR 120-130 Amendments to the International Traffic in Arms Regulations 04/07

- RM-DCFO-FPRA-FPMC Final Rule CFR 17 Overpayments From the Foreign Service Retirement and Disability Fund 03/27.doc

- RM-DCFO-FPRA-FPMC Final Rule 22 CFR 34 Debt Collection 03/27

For 2007

56838.326

- A-ISS-IPS-PP Final Rule 22 CFR 9 National Security Information Regulations 5/31/2007

- A-ISS-IPS-PP Final Rule 22 CFR 171.14 Search Fees in Freedom of Information Act Cases 10/05

- A-OPE Final Rule 1400-AC34 48 CFR Parts 601-653 DOSAR Technical Amendments 7/08

- A-OPE Proposed Rule 22 CFR Parts 639 and 652 DOSAR Security Issues for Information Technology Systems 6/6

- A-OPE-FA Final Rule 22 CFR Part 601 Department of State's Implementation of OMB Guidance on Nonprocurement Debarment and Suspension 02/05

- A-OPE Proposed Rule 48 CFR Parts 604-637-652 DOSAR HSPD Implementation 11/14

- CA-EX Interim Final Rule CFR Part 22 Schedule of Fees for Consular Services Department of State 12/14

- CA-EX Interim Final Rule CFR Part 41 Visas-Documentation of Nonimmigrants Under the Immigration and Nationality Act 12/18

- CA-OCS-PRI Final Rule 22 CFR Part 99 Intercountry Adoption - Reporting on Non-Convention and Convention Adoptions of Immigrating Children 02/26

- CA-OCS-PRI Final Rule 22 CFR Part 72 Death and Estates 02/22

- CA-PPT-LA Final Rule 22 CFR Parts 22 and 51 Card Format Passport Changes to Passport Fee Schedule 12/21

- CA-PPT-LA Final Rule 22 CFR Part 51 Passports (Final Global PPT Regs) 11/13

- CA-PPT-LA Interim Final Rule 1400-AC23 22 CFR Part 51 Passports (WHTI Surcharge Increase) 12/6

- CA-PPT-LA Interim Final Rule 1400-AC39 22 CFR Parts 22 and 51 Expedite Passport Fee Rule 08/13

- CA-PPT-LA Proposed Rule 1400-AC28 22 CFR Part 51 Passports 03/01

- CA-PPT-LA Proposed Rule 1400-AC41 22 CFR Parts 22 and 51 Security Surcharge 11/28

- CA-VO-L-R Final Rule 1400-AB49 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended 12/26

- CA-VO-L-R Final Rule 1400-AC40 Hague Convention on Intercountry Adoption-Intercountry Adoption Act of 2000-Consular Officer Procedures in Convention Cases 10/23

- CA-VO-L-R Final Rule No RIN CFR 22 Parts 41 and 42 Classification Symbols Revised 10/16

- ECA-EC-ECD Interim Final 1400-AC15 22 CFR Part 62 Exchange Visitor Program -Trainees and Interns 06/14

56838.328

- ECA-EC-EVP Final Rule 1400-AC29 22 CFR Part 62 Exchange Visitor Program -Sanctions and Terminations 12/14

- ECA-EC-ECD Proposed Rule 1400-AC30 22 CFR Part 62 Exchange Visitor Program -Secondary School Students 05/24

- ECA-EC-EVP Final Rule 1400-AC38 22 CFR Part 62 Exchange Visitor Program - Fees and Charges for Exchange Visitor Program Services 10/30

- ECA-EC-EVP NPRM 1400-AC35 22 CFR Part 62 Post Secondary Student Intern 07/31

- PM-DTC Final Rule No RIN 22 CFR Part 126 Amendment of the International Traffic in Arms Regulations Policy with Respect to Somalia 02/05

- PM-DTC Final Rule No RIN 22 CFR Part 126 Amendment of the International Traffic in Arms Regulations Policy with Respect to Vietnam 02/05

- PM-DTC Final Rule No RIN 22 CFR Part 126 Amendment of the International Traffic in Arms Regulations -UN Embargoed Countries 12/11

- PM-DTCM Final Rule No RIN 22 CFR Part 127 Voluntary Disclosures 12/07

- PM-DTCP Final Rule No RIN 22 CFR Part 121 Amendment to the International Traffic in Arms Regulations-Designation of Missile Technology Control Regime Annex 7/31

- PM-DTCP Final Rule No RIN 22 CFR Part 121 and 123 Amendment to the International Traffic in Arms Regulations-US Munitions List 7/11

56838.329

- PM-DTCP Final Rule No RIN 22 CFR Part 124 Amendment to the International Traffic in Arms Regulations Regarding Dual and Third Country Nationals 11/19

- PM-DTCP Final Rule No RIN 22 CFR Part 126 Amendment to the International Arms Traffic in Arms Regulations - United Nations Embargoed Countries 10/12

For 2008

- CA-EX Interim Final Rule 22 CFR Part 22 Schedule of Fees for Consular Services Department of State 01/21

- CA-OCS-PRI Final 22 CFR Part 7 and Part 50 Board of Appellate Review; Review of Loss of Nationality 10/09

- CA-OCS-PRI Final Rule 22CFR Part 94 Procedures for Children abducted to the United States 09/19

- CA-OCS-PRI Interim Final 22 CFR Part 7 and Part 50 Board of Appellate Review; Review of Loss of Nationality 07/15

- CA-OCS-PRI Interim Final Rule 22CFR Part 94 Procedures for Children abducted to the United States 10/27

- CA-PPT-LA Final Rule 22 CFR Part 51 Passports (Final Global PPT Regs) 01/17

- CA-VO-L-R Final Rule 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended 01/15

- CA-VO-L-R Final Rule 22 CFR 42 33 Electronic Diversity Visa 12/12

56838.330

- CA-VO-L-R Final Rule 22 CFR Part 41 Visas - Aliens Inadmissible Under the Immigration and Nationality Act – Traffickers in Persons 08/21

- CA-VO-L-R Final Rule No RIN 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended Exempt Burmese Diplomats 09/25

- CA-VO-L-R Final Rule 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended JADE Act 08/15

- CA-VO-L-R Final Rule No RIN 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended-Fingerprints 6/20

- CA-VO-L-R Final Rule 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended-Photo Requirement 02/27

- CA-VO-L-R Final Rule 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended-Procedure for Notifying the Beneficiary

- CA-VO-L-R Final Rule 22 CFR Part 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, As Amended-Offer Completely Electronic Application Procedure

- CA-VO-L-R Final Rule 22 CFR Parts 40 and 41 Visas-Documentation of Nonimmigrants under the Immigration and Nationality Act, as Amended 03/17

- CA-VO-L-R Final Rule 22 CFR Parts 40 Uncertified Foreign Health-Care Workers 10/09

56838.331

- CA-VO-L-R Final Rule CFR Parts 41 & 42 Visas-Documentation of Immigrants and Nonimmigrants-Visa Classification Symbols 04/24

- ECA-EC-AG Final Rule 22 CFR Part 62 Final Rule Post Secondary Student Intern 06/13

- ECA-EC-AG Final Rule 22 CFR Part 62 Exchange Visitor Program – Au Pairs 6/13

- ECA-EG-AG Final Rule 22 CFR Part 62 Exchange Visitor Program– College and University Students_Student Interns 8/18

- PM-DTC Final Rule 22 CFR Part 123 Amendment to the International Arms Traffic in Arms Regulations-Temporary Export Exemption for Body Armor 08/18

- PM-DTC Final Rule 22 CFR Part 123 Amendment to the International Traffic in Arms Regulations- North Atlantic Treaty Organization (NATO) 03/20

- PM-DTC Final Rule 22 CFR Part 126 Amendment to the International Arms Traffic in Arms Regulations - Sri Lanka 03/19

- PM-DTC Final Rule 22 CFR Part 121 Amendment to the International Traffic in Arms Regulations - Rwanda 09/22

- PM-DTC Final Rule 22 CFR Part 121 Amendment to the International Traffic in Arms Regulations - The US Munitions List 08/28

56838.332

- PM-DTC Final Rule 22 CFR Part 121 Amendment to the International Traffic in Arms Regulations-Section 125.4(b)(9) Export Exemption for Technical Data 08/28

- PM-DTC Final Rule 22 CFR Part 126 Amendment to the International Arms Traffic in Arms Regulations- Eritrea 08/28

- PM-DTC Final Rule 22 CFR Part 126 Cancer Drugs ITAR Change 09/15

- PM-DTC Final Rule 22 CFR Parts 121 and 129 Amendment to the International Traffic in Arms Regulations - Registration Fee Change 09/22

- PM-DTC Interim Final Rule 22 CFR Parts 122 and 129 Amendment to the International Traffic in Arms Regulations - Registration Fee Change 06/01

For 2009

- A-OPE Final Rule DOSAR HSPD-12 8/28.doc

- CA-VO-L-R Final Rule 22 CFR 42 33 Electronic Diversity Visa 03/09

- CA-PPT Final Rule Parts 22 & 51 CFR Passport Procedures-Amendment to Expedited Passport Processing Regulation 7/20

- CA-VO-L-R Final Rule 22 CFR Parts 22 & 51 CFR Visas-Documentation of Nonimmigrants Under the Immigration and Nationality Act - As Amended; Requirements for Aliens in Religious Occupations 10/1

- CA-VO-L-R Final Rule 22 CFR Parts 41 & 42 Visas Documentation of Immigrants and Nonimmigrants --Visa Classification Symbols 11/20

56838.333

- CA-EX Final Rule Schedule of Fees for Consular Services, Department of State and Overseas Embassies and Consulates-Surcharge Increase 06/26

- CA-EX Proposed Rule Schedule of Fees for Consular Services-Nonimmigrant Visa Application and Border Crossing Card Processing Fees 12/9

- CA-VO-L-R Final Rule 22 CFR 41 Foreign Officials of Immediate Family Members, As Amended 7/17

- Proposed Rule 22 CFR Part 22 Schedule of Fees for Consular Services, Department of State and Overseas Embassies and Consulates - Machine Readable Visa 12/9

- ECA-EVP Final Rule AuPair 3/16

- ECA-EVP Proposed Rule 22 CFR Part 62 Exchange Visitor Program - Subpart A, General Provisions 9/17

- ECA ANPRM Rule 22 CFR 62 EVP-Secondary School Students 8/27

- PM-DDTC Final Rule 22 CFR Parts 123, 124,126 and 129 Amendment to the International Traffic in Arms Regulations: Congressional Certification Regarding South Korea 7/28

- PM-DDTC Final Rule 22 CFR Part 126 Amendment to the International Traffic in Arms Regulations: North Korea 11/24

- PM-DDTC Final Rule 22 CFR Part 120 Amendment to the International Traffic in Arms Regulations: Defense Service Definition 6/15

56838.334

- PM-DDTC Final Rule 22 CFR Part 125 Amendment to the International Traffic in Arms Regulations: Section 125.4(b)(9) Export Exemption for Technical Data 11/2

- PM-DDTC Final Rule 22 CFR Part 126 Amendment to the International Traffic in Arms Regulations: transfer programs and foreign owned military aircraft and naval vessels 11/13

For 2010 through May 26th.

- CA-EX Proposed Rule RIN 22 PART 22 Schedule of Fees for Consular Services-Department of State and Overseas Embassies and Consulates-Adjustments in Current Fees for Consular Services; COSS Study 02/04

- CA-EX Proposed Rule RIN 22 PART 22 Schedule of Fees for Consular Services-Department of State and Overseas Embassies and Consulates-Supplemental Proposed Rule (1400-AC57 & 1400 AC58) 3/19

- CA-EX Interim final rule 22 CFR Part 22 Schedule of Fees for Consular Services, Department of State and Overseas Embassies and Consulates - Nonimmigrant Visa and Border Crossing Card Application Processing Fees 5/17

- ECA Proposed Rule 22 CFR 62 EVP - Secondary School Students 4/27

- PM-DDTC Final Rule PARTS 124-126-129 ITAR-Congressional Certification Regarding South Korea 3/24

- PM-DDTC Final Rule PARTS 124-126-129 ITAR-Removing Requirement for Prior Approval Relating to Significant Military Equipment 3/24

- PM-DDTC Final Rule RIN PART 120 Amendment to the International Traffic in Arms Regulations-Commodity Jurisdiction 01/25

56838.335

- PM-DDTC Final Rule RIN PARTS 120-121-123-126 Amendment to the ITAR_North Atlantic Treaty Organization Definition and Other Administrative Corrections 02/19

- PM-DDTC Final Rule RIN PART 126 Amendment to the International Traffic in Arms Regulations_Sri Lanka 02/02

56838.336

Question#:	6
Topic:	intell
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Mr. Russell E. Travers, the Deputy Director, of Information Sharing and Knowledge Development, National Counterterrorism Center (NCTC), Office of the Director of National Intelligence testified to the Homeland Security and Governmental Affairs Committee (HSGAC) on March 10, 2010 that NCTC is having some success with some departments and not so much success with others in "ingesting" intelligence information that could help secure our country.

Are you having any issues in accessing the information you need to carry out your security investigations of the visa application process effectively? If so, what issues are you having?

How would you recommend fixing the issues?

Response: The Visa Security Program (VSP) recently placed personnel at the U.S. Customs and Border Protection's (CBP) National Targeting Center and at the National Counterterrorism Center (NCTC) to enhance access to and sharing of information. VSP continually seeks better access to information and has recently participated in NCTC's Inter-Agency Coordination Group to improve VSP's access to FBI data. Access to CBP's Passenger Name Record data has also proven valuable in the past. Additionally, VSP continues to modernize its case management system and is seeking to automate links with the Department of State and to expand the scope and quality of data against which visa applicants are checked.

56838.307

Post-Hearing Questions for the Record
Submitted to the Honorable David F. Heyman and the Honorable John T. Morton
From Senator Susan M. Collins

"The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process"
April 21, 2010

Question#:	7
Topic:	TIDE
Hearing:	The Lessons and Implications of the Christmas Day Attack: Securing the Visa Process
Primary:	The Honorable Susan M. Collins
Committee:	HOMELAND SECURITY (SENATE)

Question: Under current law, including section 428 of the Homeland Security Act of 2002, does the Secretary of Homeland Security have the authority to establish a visa policy that would require that the visas of all persons in the TIDE database be revoked pending further investigation?

Response: Section 428(b)(1) of the Homeland Security Act provides that the Secretary of Homeland Security "shall have the authority to refuse visas in accordance with law and to develop programs of homeland security training for consular officers (in addition to consular training provided by the Secretary of State), which authorities shall be exercised through the Secretary of State, except that the Secretary shall not have authority to alter or reverse the decision of a consular officer to refuse a visa to an alien . . . ."

In September 2003, Secretary of Homeland Security Ridge and Secretary of State Powell signed a memorandum of understanding (MOU) regarding the implementation of Section 428 of the Homeland Security Act. Under the MOU, "DHS will have authority to issue or approve (hereinafter 'final responsibility over') visa guidance, except for those matters that are the specific responsibility of the Secretary of State as prescribed in section 428(c)(2) and (d)(2) of the Act, in existing statutes related to foreign policy or management of the visa process, in future statutes, Presidential proclamations and executive orders. . . ." DHS is required under the MOU to provide notice to DOS when it begins drafting rules, policies or procedures affecting the visa process and also must offer DOS the opportunity to consult regarding security, legal, operational, resource, or foreign policy or foreign relations issues. The MOU expresses a preference for joint DHS-DOS rulemakings that affect the visa process.

In response to the December 25, 2009 attempted bombing, on December 27, 2009, President Obama ordered reviews of airport security measures and watch-list policies to determine if there are specific areas that warrant change or significant modifications. DHS is working with inter-agency partners to re-evaluate the criteria and processes used.

56838.308

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Daniel K. Akaka (#1)
Senate Committee on Homeland Security
April 21, 2010

Question:

I am a strong supporter of the Visa Waiver Program (VWP), which facilitates and encourages foreign travel to the U.S. for both business and pleasure. Waiving the visa requirement for low-risk, high-volume countries may reduce the workloads in these particular consular offices and allow for a concentration of consular resources for the greater-risk nations in the visa process.

Has the VWP allowed the Department of State to shift attention from high-volume/low-risk nations to greater-risk nations? If so, please describe how the Department is handling this shift in terms of additional workforce training and language proficiency skills at these new posts? If not, please discuss why you believe this is, as well as how the Department is planning for any anticipated changes in workload.

Answer:

Yes, the VWP has allowed the Department to shift resources to better manage visa volume and risk. Each year the Bureau of Consular Affairs conducts a review of workload and staffing at our consular sections overseas. We take into consideration the types of consular work conducted at post, its complexity, and the security environment. We use this review to conduct a repositioning exercise whereby we transfer consular positions from sections that show a surplus of officer staff to consular sections that are understaffed.

56838.339

In recent years, the majority of the positions that we have repositioned come from posts that have recently entered the Visa Waiver Program. For example, 13 consular positions have moved, or are being moved, out of Seoul, Korea, to other consular sections. The position typically moves when the incumbent officer at a post departs at the end of his/her scheduled tour.

The Bureau of Consular affairs also participates in a Department-wide review of language designations for existing positions and recommends changes as appropriate. When a consular position is repositioned to a new consular section, the appropriate language designation for the position is added. For example, one of the positions in Seoul has been repositioned to the Consulate General in Ciudad Juarez. The position in Ciudad Juarez requires fluency in Spanish.

56838.340

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#1)
Senate Committee on Homeland Security
April 21, 2010

Question:

Unlike many other countries that have a dedicated consular function, consular officers at the State Department are generally junior Foreign Service officers in their first or second deployment. The Committee is concerned that we are sending these junior Foreign Service officers to adjudicate visas in high-risk posts, in parts of the world where we know full well that the threat of Islamist extremism is pervasive and there are terrorists probing our defenses constantly trying to get through.

Can you explain to the Committee the rationale behind sending junior Foreign Service officers to adjudicate visas at high-risk posts?

Answer:

The Department believes that filling Consular Officer positions from the wider Foreign Service Officer workforce is the best means of placing highly qualified, highly trained, and highly motivated professionals in visa adjudication positions around the world. In their careers, Foreign Service Officers serve in variety of posts and gain valuable professional experience working in different countries and gaining facility in a host of languages. Officers beginning their foreign affairs careers are fully prepared and closely supervised by experienced officers who review adjudications every day and contribute their years of experience to the mentoring and supervision of those entry-level officers.

56838.341

Consular officers have the foreign language skills necessary to stay abreast of local trends and conduct visa interviews: 1,067 of our consular officer positions require fluency in one of 65 local languages. Each consular officer is required to complete the Department's 31-day 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 namechecking technique training, as well as fraud prevention. Officers who choose consular work as their career path receive continuing education, including courses in analytic interviewing, fraud prevention, and advanced security namechecking.

We support consular officers with additional personnel, the latest technology, and access to advanced screening tools and information systems. In the field, consular officers are supported by 3,953 locally engaged staff and 75 full-time Assistant Regional Security Officer Investigators – soon to increase by up to 48 additional positions —specifically devoted to maintaining the integrity of the visa process. Seven Regional Consular Officers, who are experienced visa adjudicators and managers, use regular visits and daily electronic contact to provide an additional level of oversight, mentoring, and guidance to small, isolated consular sections in various regions. Experts in the Bureau of Consular Affairs in

56838.342

Washington, D.C., provide legal, regulatory, and policy support to the field. We also have a large Fraud Prevention Programs office that works very closely with the Bureau of Diplomatic Security, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center and the National Visa Center in Portsmouth, New Hampshire.

56838.343

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#2)
Senate Committee on Homeland Security
April 21, 2010

Question:

How do the security measures for issuing visas that are in place at the 57 high-risk consular posts jointly identified by DHS and State differ from those at other posts?

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 threat and other information.

56838.344

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#3)
Senate Committee on Homeland Security
April 21, 2010

Question:

When a consulate learns that a person may be linked to terrorism, they send a "Visas Viper" cable to the National Counterterrorism Center. In the Abdulmutallab incident, the Visas Viper cable from the U.S. Embassy in Abuja contained sparse details about the information the post received from Mr. Abulmutallab's father. The only person at the Embassy to interview the father was reportedly a CIA agent assigned there.

Had a Visa Security Unit been stationed in Nigeria, would the ICE agents assigned there have been involved in the interview with the father and the cables that were subsequently sent out?

Answer:

Given the nature of the original meeting with the father, it is a fair assumption that an ICE agent would not have been involved. An ICE agent would have received a copy of the Visas Viper cable, which was communicated widely throughout the USG law enforcement and intelligence community, including ICE, in Washington.

56838.345

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#4)
Senate Committee on Homeland Security
April 21, 2010

Question:

Please provide the Committee with any documents State has that detail the exact changes to the Visas Viper process that have resulted from the President's Review.

Answer:

The following are provided:

STATE 132497: VISAS VIPER - INCLUDING VISA INFORMATION

STATE 002602: REQUEST FOR POSTS TO HOLD EAC MEETINGS TO REVIEW TERRORISM ISSUES INCLUDING VISAS VIPER

STATE 047555: NEW POLICIES AND PROCEDURES ON THE VISAS VIPER INTERAGENCY TERRORIST REPORTING PROGRAM

9 FAM 40.37 and exhibits updated

(Please note that some of these items are sensitive and not for public release.)

56838.346

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#5)
Senate Committee on Homeland Security
April 21, 2010

Question:

The Committee continues to be concerned that we do not have an automated system for ensuring that a traveler's visa status is verified electronically as they check in for their flight. Although the airlines are charged with checking a traveler's documents, but obviously in the case of a revoked visa the document does not tell the whole story. This is disconcerting because it means that a traveler with a revoked visa could board an airplane to the United States.

Is all visa revocation information immediately made electronically available/accessible to airlines and CBP officers?

Answer:

We work closely with CBP to ensure that airlines are aware of any travelers with revoked visas prior to boarding. When the State Department revokes a visa, a "VRVK" revocation code is entered into the Consular Lookout and Support System (CLASS), our online repository of visa lookout records. The VRVK entry automatically replicates to DHS's equivalent TECS lookout database. Currently, as part of its enhanced "No Board" initiative, DHS CBP uses these VRVK records, among other lookout codes, to advise airlines that certain passengers should not be boarded on flights bound for the United States.

56838.347

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#6)
Senate Committee on Homeland Security
April 21, 2010

Question:

What is the current timeline for having an electronic visa revocation check done as passengers board an airplane?

Answer:

The State Department supports ongoing CBP efforts to implement an updated, universal electronic system of notification to airlines. We respectfully refer you to CBP for more specific information.

56838.348

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#7)
Senate Committee on Homeland Security
April 21, 2010

Question:

Please provide the Committee with a copy of the President's Directive for Visa Revocations and with any other documents explaining changes to the visa revocation process that have resulted from the President's Review.

Answer:

In the Presidential Memorandum Regarding (the) 12/25/2009 Attempted Terrorist Attack, issued on January 7, 2010, the President directed the Department of State to review visa issuance and revocation criteria and processes, with special emphasis on counterterrorism concerns, and determine how technology enhancements can facilitate and strengthen visa-related business processes.

Since the Presidentially ordered Security Review, which directed multiple U.S. Government agencies to take actions to enhance the security of the American people, there were exigent changes in the thresholds for adding individuals to the Terrorist Screening Database (TSDB), No-fly, and Selectee lists, and the number of revocations increased substantially as a result. Since the 12/25 attack we have revoked hundreds of visas under P3B (prospective terrorist) grounds because the

56838.349

aliens' names were added to the above-referenced databases. Given the fluid nature of the exigent changes referred to above, we cannot say with precision how many of these revocations directly resulted from the TSDB scrub. However, we can say that the vast majority of the revocation subjects – which included in addition to the "scrub," normal referrals from posts, the Terrorist Screening Center, and Customs and Border Protection – were individuals who met TSDB criteria.

We are providing the following documents to you under separate cover as these items are not for public release.

PRESIDENTIAL MEMORANDUM REGARDING 12/25/2009 ATTEMPTED TERRORIST ATTACK

STATE 047555: NEW POLICIES AND PROCEDURES ON THE VISAS VIPER INTERAGENCY TERRORIST REPORTING PROGRAM

STATE 11763: POST-DECEMBER 25 PRUDENTIAL VISA REVOCATIONS

(Note: the above is a classified cable and will need to be forwarded accordingly.)

56838.350

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#8)
Senate Committee on Homeland Security
April 21, 2010

Question:

The Committee has long advocated for increased intelligence and information sharing between federal agencies. Tremendous strides have been taken in this arena by State and DHS, and consular officers check a wide range of databases when making their determinations. Nevertheless, the Committee has been made aware of complaints from consular officers that there are some databases that they do not have full access to. Does the Department of State believe that it has access to all of the law enforcement and watch list information it needs to properly manage the visa process?

Answer:

Consular officers have access to all of the law enforcement and watchlist information they need in order to properly screen visa applicants. Names of visa applicants are checked against the Consular Lookout and Support System (CLASS), which has over eleven million records from the FBI, six million from the Department of Homeland Security (DHS), and over 400,000 names of known or suspected terrorists (KSTs) from the Terrorist Screening Center. Visa applicant fingerprints are searched against the DHS Automated Biometric Identification System (IDENT) fingerprint system, which contains all available fingerprints of KSTs, as well as fingerprints of wanted persons and immigration law violators. Visa applicant fingerprints are also checked against the FBI IAFIS fingerprint

56838.351

system, which contains over 50 million criminal history records. The checks against CLASS, IDENT, and IAFIS are fully automated components of the visa issuance process. All consular posts now have access to CBP's Arrival and Departure Information System (ADIS) and we are working with DHS for wider access to CLAIMS and ENFORCE. Sometimes screening checks may find a reference to a record that is not fully available yet online, but such records can be obtained through an email request. While this is not a visa screening vulnerability because the lookout record is contained in the screening system, we are continuing our system integration efforts to make all such background records available online to eliminate the need for such email requests.

56838.352

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#9)
Senate Committee on Homeland Security
April 21, 2010

Question:

Regarding the Visa Security Program, what information (automated or otherwise) is available to ICE agents, but not to consular officers, during the visa adjudication process?

Answer:

We are unaware of any database that an ICE agent would check that would contain data not available to a consular officer. We know that ICE agents screen visa applicant names against the DHS TECS system, but according to longstanding cooperation between CLASS and TECS management, any records in TECS that would have a bearing on visa eligibility should already be transferred to CLASS through fully automated data transfer processes currently in effect on the CLASS-TECS interface. The information sharing process put in place following the September 11, 2001, terrorist attacks requires a full sharing of relevant information by all agencies.

Consular officers have access to a wide range of interagency material. In addition to a search of the Consular Consolidated Database conducted to find any previous visa applications, consular officer screening of visa applicants consists of

56838.353

four major components. First are name checks against the Consular Lookout and Support System (CLASS), which has over eight million Department of State (DOS) records, over eleven million records from the FBI, six million from the Department of Homeland Security (DHS), and over 400,000 names of known or suspected terrorists (KSTs) from the Terrorist Screening Center. Secondly, visa applicant fingerprints are searched against the DHS IDENT fingerprint system, which contains all available fingerprints of KSTs, as well as fingerprints of wanted persons and immigration law violators. Visa applicant fingerprints are also checked against the FBI IAFIS fingerprint system, which contains over 50 million criminal history records. Third, photos of visa applicants are checked against the DOS Facial Recognition System, which contains over 100,000 photos of KSTs received from the Terrorist Screening Center, in addition to over 85 million photos of previous visa applicants. Fourth, for cases of special concern consular officers must send a Security Advisory Opinion request to Washington to be reviewed by the Department of State and law enforcement and intelligence agencies.

56838.354

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#10)
Senate Committee on Homeland Security
April 21, 2010

Question:

In the eight years since the creation of the Visa Security Program, only 14 of the more than 200 consular posts that issue visas have received Visa Security Units. A joint DHS-State study resulted in a plan for implementing the program at all 57 high risk consular posts by 2013. Given the slow pace of implementation, and the fact that the FY2011 budget does not include any new funding for continuing to expand the program, this no longer seems likely.

When does State believe that the Visa Security Program will be deployed to all of the 57 high-risk posts identified by the joint DHS-State review?

Answer:

The schedule for Visa Security Unit (VSU) deployment is subject to budget and resource realities. We understand that in FY 2010, ICE received funding that will be used to deploy to four additional posts this year as well as to expand positions in two existing posts. (The requisite National Security Decision Directive 38 (NSDD-38) requests for the four new VSUs and one of the two expansion requests have been approved by the posts' Chiefs of Mission.) For FY 2011, the President has requested the same level of funding and resources as FY 2010, which will cover existing VSUs, (including the planned locations and positions from the FY 2010 expansion), and will establish a new office in Saudi Arabia. We were advised that ICE is continuing Visa Security Program (VSP)

56838.355

deployment in accordance with its five-year VSP Expansion Plan, which received approval and support across the Department of Homeland Security, the Department of State, and the White House Homeland Security Council. For additional information regarding VSP expansion, we refer you to DHS/Immigration and Customs Enforcement.

56838.356

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#11)
Senate Committee on Homeland Security
April 21, 2010

Question:

What are the main reasons for the slow pace of expansion?

Answer:

The schedule for Visa Security Unit (VSU) deployment is subject to budget and resource realities. We understand that in FY 2010, ICE received funding that will be used to deploy to four additional posts this year as well as to expand positions in two existing posts. (The requisite National Security Decision Directive 38 (NSDD-38) requests for the four new VSUs and one of the two expansion requests have been approved by the posts' Chiefs of Mission.) For FY 2011, the President has requested the same level of funding and resources as FY 2010, which will cover existing VSUs, (including the planned locations and positions from the FY 2010 expansion), and will establish a new office in Saudi Arabia. We were advised that ICE is continuing Visa Security Program (VSP) deployment in accordance with its five-year VSP Expansion Plan, which received approval and support across the Department of Homeland Security, the Department of State, and the White House Homeland Security Council. For additional information regarding VSP expansion, we refer you to DHS/Immigration and Customs Enforcement.

56838.357

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Joseph I. Lieberman (#12)
Senate Committee on Homeland Security
April 21, 2010

Question:

It is our understanding that a number of Ambassadors have notified DHS in the past several years that they would not endorse a VSP office at their Embassy. Please provide the Committee with an explanation of each instance since the creation of the program that this has occurred. Additionally, please provide a detailed explanation of what State plans to do in the future to ensure that the program is expanded to all 57 high risk posts in an expedited manner.

Answer:

ICE's initial difficulties in delineating a unique mission for its VSU program, considered by individual Chiefs of Mission (COM) in the context of their NSDD-38 responsibilities, led COMs in Kuala Lumpur, Nairobi, London, and Astana (for Istanbul) to resist the placement of VSUs at their missions. In Manila, Islamabad, and Jakarta initial COM reservations were overcome and VSUs were established. Often the justification put forward by ICE focuses heavily on other ICE responsibilities and not on the VSP.

In Kuala Lumpur, the COM denied an NSDD-38 request for three officers to supervise or conduct criminal investigations. Kuala Lumpur is a low-fraud post, and law enforcement and security personnel at post are not aware of visa security issues that could engage three criminal investigators. In addition, the Malaysian

56838.358

government does not permit U.S. law enforcement officers to conduct independent investigations of Malaysian citizens. Any such investigations would have to be conducted jointly, and the Malaysians would be unlikely to do so without existing evidence of criminal activity.

In Nairobi, DHS requested two VSU positions, while the COM asked ICE to fill a long-vacant GS-14 position and said he would reassess the VSU request after one year. In January 2008, the COM initiated a proposal to abolish the still-vacant GS-14 position. In May 2008, ICE informed the COM that it was closing the ICE operation because the COM had not approved the two VSU positions; ICE decided to close the operation after determining that it could not cover its operations in Nairobi with its single existing position.

In London, initial difficulties in defining the unique roles and responsibilities of the Visa Security Program have been overcome, and a VSU is due to open this year. In early June a joint DOS-DHS team visited Ankara (as well as Beirut, Lebanon) to discuss the establishment of a VSU in Ankara and/or Istanbul.

Regarding further expansion of the program, the Department of State works collaboratively with DHS pursuant to an October 2004 *Memorandum of Understanding between the Department of State and the U.S. Immigration and Customs Enforcement, Visa Security Unit (ICE/VSU) on the Administrative*

56838.359

Aspects of Assigning Personnel Overseas, and NSDD-38 to determine where the establishment of a VSU is appropriate. Department officers are assigned to work with ICE on site selection and setting up VSUs overseas, as well as navigating the interagency process for establishing new positions overseas. Over the years, the Department has gone to extraordinary lengths to support ICE/VSU expansion, including sending senior consular and diplomatic security officers on visits to posts to help ICE officers explain their mission to Chiefs of Mission.

56838.360

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Susan M. Collins (#1)
Senate Committee on Homeland Security
April 21, 2010

Question:

Your statement discussed the government's review of the terrorist screening database (TSDB) after the attempted attack on December 25, 2009, to identify individuals with valid U.S. visas that should be revoked. The GAO has informed the Committee that 1,150 persons identified in this review had valid visas. Please confirm the number of individuals on the TSDB who had valid U.S. visas that the review identified, provide the number of individuals who had their visas revoked as a result of this review, and provide an explanation for why any individuals on that list have visas that have not been revoked (e.g., waivers for law enforcement or other investigative reasons).

Answer:

The action cited above concerns an interagency review of all visa holders listed in the Terrorist Identities Datamart Environment (TIDE) database, which feeds the TSDB. All of these individuals were temporarily placed on the No-Fly List pending "deep-dive" reviews of each case by the intelligence and law enforcement communities. Visa revocation recommendations are made by the TSC to the State Department on a case-by-case basis as the deep-dive reviews are completed. In many instances, the intelligence review has led to the individual being downgraded from the No-Fly List to Selectee or another status. These lists are under constant review and are changing frequently, so any statistics represent a

56838.361

"snapshot" in time. We refer you to the Terrorist Screening Center for the most up to date reports on this ongoing interagency effort.

Between December 26, 2009, and June 2, 2010, the Department revoked over 630 visas on terrorism-related grounds. The revocation subjects included referrals from posts abroad, the Terrorist Screening Center, and Customs and Border Protection in addition to cases associated with the post-12/25 review effort.

There are several reasons why an individual may by included in the TSDB and still hold a valid visa, including: 1) law enforcement or other investigative concerns, 2) recent completion of an interagency Security Advisory Opinion with a review of all available information included in TIDE, 3) granting of a DHS waiver of ineligibility, and 4) activity or conduct that would warrant watchlisting in the TSDB might not reflect a threat and be considered sufficient to justify denial of a visa or admission to the U.S. under the Immigration and Nationality Act (INA).

It should be noted that the TSDB watchlist is not, and was never intended to be, an exclusion list precluding entry to the United States. It is intended to alert screening agencies that there is information in the U.S. government's possession that should be reviewed as part of the screening process.

56838.362

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Susan M. Collins (#2)
Senate Committee on Homeland Security
April 21, 2010

Question:

Your testimony referred to cable guidance to consular posts on the new procedures to be followed in submitting Visas Vipers from consular posts. Please provide a copy of this guidance.

Answer:

The following documents are provided to you under separate cover.

STATE 132497: VISAS VIPER - INCLUDING VISA INFORMATION

STATE 002602: REQUEST FOR POSTS TO HOLD EAC MEETINGS TO REVIEW TERRORISM ISSUES INCLUDING VISAS VIPER

STATE 047555: NEW POLICIES AND PROCEDURES ON THE VISAS VIPER INTERAGENCY TERRORIST REPORTING PROGRAM

(Please note that some of these items are sensitive and not for public release.)

9 FAM 40.37 and exhibits updated

(Please note that some of this guidance is sensitive and not for public release.)

56838.363

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Susan M. Collins (#3)
Senate Committee on Homeland Security
April 21, 2010

Question:

You testified that software upgrades on State Department computers at consular posts will contain algorithms to implement "fuzzy logic" so that name searches will automatically produce similar name spellings in the Department's Consular Consolidated Database. Please provide the timeline for implementing this upgrade.

Answer:

New visa applicants are automatically searched against the Consular Consolidated Database (CCD) to determine if they have previous visa applications on file. In order to enhance this process, the Bureau of Consular Affairs developed a modification to apply a fuzzy logic to these searches of the CCD. The fuzzy logic has now been deployed and is in use worldwide for automated searches of records in the CCD for all visa applicants. For searches outside the context of a visa application, Consular Officers have been instructed to use our "Person Finder" fuzzy search application.

56838.364

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Claire McCaskill (#1)
Senate Committee on Homeland Security
April 21, 2010

Question:

In your opening testimony, you mentioned that the Department of State (DOS) is hiring 48 additional investigator positions to work in consular sections overseas. Are any of these investigators going to the 57 high-risk posts identified by DOS and the Department of Homeland Security (DHS) under the Visa Security Program (VSP)? If so, how many of them will be going to the remaining 43 high-risk posts where Immigration and Customs Enforcement (ICE) investigators are currently not present? If there are DOS investigators going to any of the 43 high-risk posts where ICE currently is not present, what are the specific issues with getting ICE investigators to those locations?

Answer:

The Department of State's Diplomatic Security Service (DSS) previously has established 75 special agent positions located in the consular sections at 71 U.S. Embassies and Consulates. These 75 DSS Special Agents are referred to as Assistant Regional Security Officer-Investigators (ARSO-I). This year, DSS has funding for up to 48 additional ARSO-I positions.

Of the current VSU posts, ARSO-Is are located in 12 of the 14 established VSUs. By the end of 2010 we will have ARSO-I positions established in the remaining two (Saudi Arabia and Hong Kong). Of the new VSUs due to open later in 2010,

56838.365

ARSO-Is are assigned to Tel Aviv, Sana'a, and London, and an ARSO-I position in Jerusalem has been established and paneled.

Regarding the projected VSU country list, DSS already has ARSO-I positions established in Turkey, Colombia, India, Mexico, Brazil, China, Peru, Thailand, Nigeria, Russia, Bangladesh, Kenya, Malaysia, Ecuador, Ethiopia, Paraguay, and South Africa. Currently, the Bureaus of Diplomatic Security and Consular Affairs are coordinating on the assignment of A/RSO-Is at posts in the remaining high-risk countries, including Algeria, Kyrgyzstan, Qatar, Tajikistan, Sudan, Kuwait, France, Bosnia, Uzbekistan, Tunisia, and possibly Berlin (in addition to the ARSO-I currently assigned to Frankfurt).

Regarding further expansion of the Visa Security Program (i.e., assigning ICE investigators to more high-risk posts), the Department of State works collaboratively with DHS pursuant to an October 2004 *Memorandum of Understanding between the Department of State and the U.S. Immigration and Customs Enforcement, Visa Security Unit (ICE/VSU) on the Administrative Aspects of Assigning Personnel Overseas, and NSDD-38* to determine where the establishment of a VSU is appropriate. Department officers are assigned to work with ICE on site selection and setting up VSUs overseas, as well as navigating the

56838.366

interagency process for establishing new positions overseas. Over the years, the Department has gone to extraordinary lengths to support ICE/VSU expansion, including sending senior consular and diplomatic security officers on visits to posts to help ICE representatives explain their mission to Chiefs of Mission.

56838.367

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Claire McCaskill (#2)
Senate Committee on Homeland Security
April 21, 2010

Question:

What is the difference between the Department of State (DOS) investigators and Immigration and Customs Enforcement (ICE) investigators? Please explain.

Answer:

Department of State's Diplomatic Security Service (DSS) Special Agents are federal law enforcement officers who have statutory authority to investigate cases of passport and visa fraud, domestically and overseas. DSS Special Agents are located in more than 200 overseas U.S. missions and in 23 domestic field offices.

As employees of a foreign affairs agency, DSS Special Agents serve at least half of their careers in the Regional Security Offices of our overseas U.S. missions. As the law enforcement and security branch of the U.S. Department of State, DSS Special Agents develop key professional relationships with our foreign law enforcement partners, not only to ensure the safety of our mission employees, but to also conduct passport and visa criminal investigations and provide training.

ARSO-I statistics from FY2004-2009:

56838.368

Arrests	3,024
Lookouts entered	7,706*
Visas refused/revoked	12,428*
Passport/Consular Report of Birth Abroad (CRBA) denied	935*
Foreign officials trained	20,290

*Through criminal investigations, ARSO-Is developed information used by consular officers to adjudicate the refusal of passports/CRBAs; to place lookouts in CA databases; and to adjudicate the refusal or revocation of visas.

ARSO-Is are DSS Special Agents assigned to work with consular sections, with a predominant responsibility to conduct criminal investigations of passport and visa matters. In addition to basic agent training at the Federal Law Enforcement Training Center and DSS Training Center, ARSO-Is receive more than one year of specialized training (foreign language, country area studies, the Basic Consular Course, Regional Security Officer Course, ARSO-I Course, and asset forfeiture training) prior to overseas assignments.

Regarding ICE investigators assigned to U.S. missions, the MOU between the Secretaries of State and Homeland Security implementing Section 428 of the Homeland Security Act of 2002 states that DHS employees assigned to overseas posts under section 428(e) perform the following duties:

56838.369

- Advise consular officers regarding specific country threats relating to the adjudication of individual visa applications or classes of applications.

- Review any such applications, either on the initiative of the DHS employee in accordance with procedures prescribed by DHS or upon request by a consular officer or other person charged with adjudicating such applications. The actions may include, but are not limited to, providing input to or recommending security advisory opinion requests based on their expertise.

- Conduct investigations with respect to consular matters under the jurisdiction of the Secretary of Homeland Security.

These activities are carried out in coordination with Consular Officers and Diplomatic Security Special Agents assigned to post, under the authority of the Chief of Mission.

56838.370

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Claire McCaskill (#3)
Senate Committee on Homeland Security
April 21, 2010

Question:

In the hearing, you stated that there have been instances where the Chief of the Mission has denied requests for a Visa Security Program (VSP). Please list the specific reasons for those instances. In each case, how are the investigative services currently being handled?

Answer:

ICE's initial difficulties in delineating a unique mission for its VSU program, considered by individual Chiefs of Mission (COM) in the context of their NSDD-38 responsibilities, led COMs in Kuala Lumpur, Nairobi, London, and Ankara (for Istanbul) to resist the placement of VSUs at their missions. In Manila, Islamabad and Jakarta initial COM reservations were overcome and VSUs were established. Often the justification put forward by ICE focuses heavily on other ICE responsibilities and not on the VSP.

In Kuala Lumpur, the COM denied the NSDD-38 request for three officers to supervise or conduct criminal investigations. Kuala Lumpur is a low-fraud post, and law enforcement and security personnel at post are not aware of visa security issues that could engage three criminal investigators. In addition, the Malaysian government does not permit U.S. law enforcement officers to conduct independent

56838.371

investigations of Malaysian citizens. Any such investigations would have to be conducted jointly, and the Malaysians would be unlikely to do so without existing evidence of criminal activity.

In Nairobi, DHS requested two VSU positions, while the COM asked ICE to fill a long-vacant GS-14 position and said that he would reassess the VSU request after one year. In January 2008, the COM initiated a proposal to abolish the still-vacant GS-14 position. In May 2008, ICE informed the COM that it was closing the ICE operation because the COM had not approved the two VSU positions; ICE decided to close the operation after determining that it could not cover its operations in Nairobi with its single existing position.

In London, initial difficulties in defining the unique roles and responsibilities of the Visa Security Program have been overcome, and a VSU is due to open this year. In early June a joint DOS-DHS team will visit Ankara (as well as Beirut, Lebanon) to discuss the establishment of a VSU in Ankara and/or Istanbul.

The schedule for Visa Security Unit (VSU) deployment is subject to budget and resource realities. We understand that in FY 2010, ICE received funding that will be used to deploy to four additional posts this year as well as to expand positions in two existing posts. (The requisite National Security Decision

56838.372

Directive 38 (NSDD-38) requests for the four new VSUs and one of the two expansion requests have been approved by the posts' Chiefs of Mission.) For FY 2011, the President has requested the same level of funding and resources as FY 2010, which will cover existing VSUs, (including the planned locations and positions from the FY 2010 expansion), and will establish a new office in Saudi Arabia. We are advised that ICE is continuing Visa Security Program (VSP) deployment in accordance with its five-year VSP Expansion Plan, which received approval and support across the Department of Homeland Security, the Department of State, and the White House Homeland Security Council. For additional information regarding VSP expansion, we refer you to DHS/Immigration and Customs Enforcement.

56838.373

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Claire McCaskill (#4)
Senate Committee on Homeland Security
April 21, 2010

Question:

On September 28, 2003, then-Secretary of State Colin Powell and then-Secretary of Homeland Security Thomas Ridge signed the memorandum of understanding (MOU) implementing §428 of the Homeland Security Act of 2002. The MOU described each department's responsibilities in the area of visa issuances. Among its major elements, the MOU stated that the Department of State (DOS) may propose and issue visa regulations subject to Department of Homeland Security (DHS) consultation and final approval.
How many of these major visa regulations have been approved since 2003? What were they?
Has DHS and DOS had any disagreements over any of the regulations? What was the outcome?

Answer:

See the attached list of 184 visa regulations approved since 2003. We have had no disagreements with DHS with respect to any of these regulations.

56838.374

Questions for the Record Submitted to
Assistant Secretary Janice L. Jacobs by
Senator Claire McCaskill (#5)
Senate Committee on Homeland Security
April 21, 2010

Question:

Mr. Russell E. Travers, the Deputy Director, of Information Sharing and Knowledge Development, National Counterterrorism Center (NCTC), Office of the Director of National Intelligence testified to the Homeland Security and Governmental Affairs Committee (HSGAC) on March 10, 2010, that NCTC is having some success with some departments and not so much success with others in "ingesting" intelligence information that could help secure our country.

Are you having any issues in accessing the information you need to carry out your security investigations of the visa application process effectively? If so, what issues are you having? How would you recommend fixing the issues?

Answer:

All applicants for U.S. visas are screened against biographic name-checking systems and biometric verification databases. In this way, the Department of State can tap into the collective resources of our partners in the intelligence community, law enforcement, and the Department of Homeland Security to ensure that any relevant information is taken into consideration when making visa decisions. In each of the past several years, this vigorous vetting of every visa application has identified over 250,000 visa applicants who require additional security screening conducted via the interagency Security Advisory Opinion process before a visa can be issued. The efficacy of this layered screening process depends upon

56838.375

information collected, analyzed and disseminated by the U.S. government law enforcement and intelligence communities. 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 our interagency partners.

Moving beyond our efforts to adjudicate individual cases to overall process improvements, we support and participate in the ongoing interagency initiative established and conducted by the National Security Staff to refine and enhance the namechecking and watchlisting processes. With regard to the NCTC specifically, we note that NCTC has full access to the Consular Consolidated Database (CCD) containing all U.S. visa records, and that the Department of State's newly revised guidance on Visas Viper procedures was reviewed by NCTC personnel before it was disseminated to the field. The Department maintains a continuing and productive dialogue with NCTC and our other interagency partners on border security issues.

○

56838.376